CPSC 329 Assignment 1
David Ng
30009245
T04

1. I would like for there to be some written documentation of what is covered in lectures. I would also like for there to be some sort of document that describes parts of the textbook that are relevant to each lecture for further reading, along with possible supplementary problems to prepare for tests.

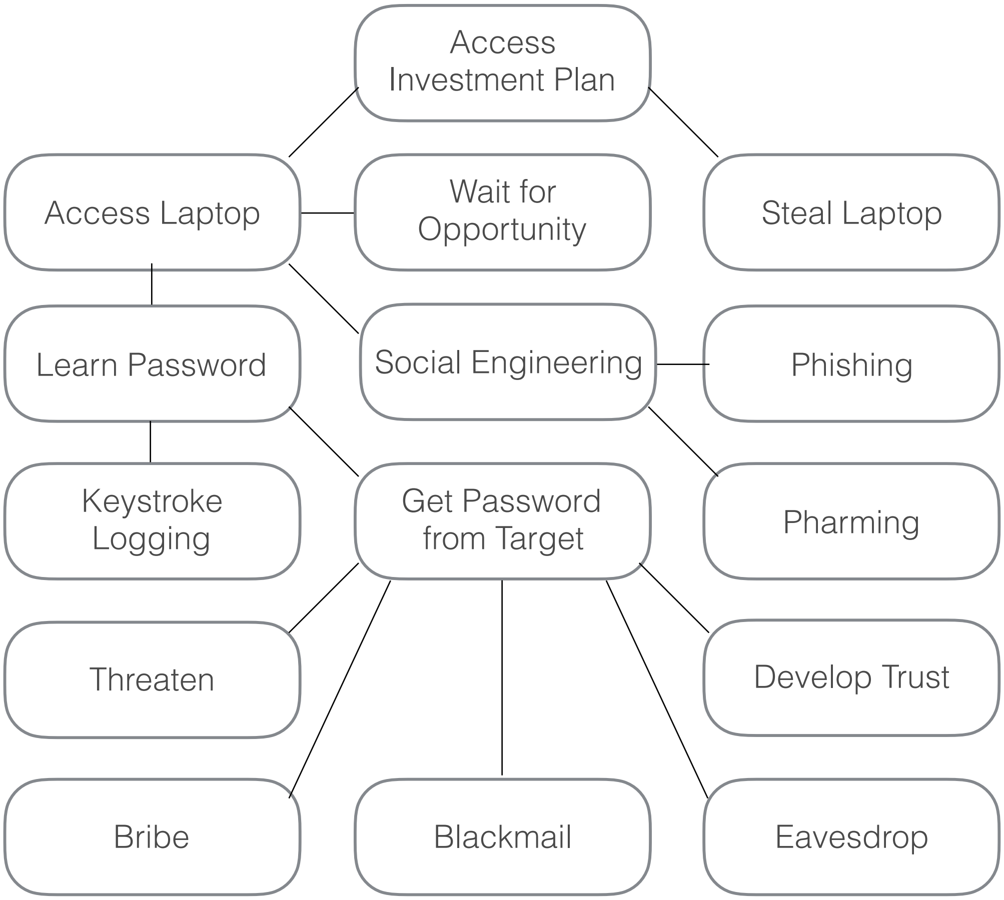
2.
    1. **Hacktivism**: Throughout last year, hacktivists launched many cyberattacks against the website of several government websites to draw attention to various issues, such as the Flint water crisis and the shooting of Michael Brown in Ferguson, Missouri. Within one week of Brown's death, Anonymous, a "relatively small vigilante cyber group", began their attack using denial of service and doxing tactics on state, local, and law enforcement officials. By targeting the main websites of state, those websites suffered brief outages that resulted in at least $150,000 in costs for services to protect those networks from the hacktivists. These types of attacks are relatively simple to detect, since they have a clearly visible result that is intended to disrupt operations in a visible manner. To fend off these attacks, IT staff quickly launched their defenses to prevent further damage. Steps were also taken to prevent future damage, such as making sure that their internet service providers install programs to help block illegitimate web traffic. Turning to global cybersecurity companies that offer their services to combat these attacks was also considered as a precautionary step. In this particular attacks, the hacktivists were motivated to spread the word and condemn those who they felt were responsible for wrongdoing. This is supported by the fact that Anonymous once again caused website outages through their attacks after a grand jury decided not to indict the officer responsible for shooting Brown. Hacktivism, defined as hacking to achieve the ends of social or political causes, is represented in this event, since the attacks were motivated by a desire to bring to attention a social injustice. By attacking the websites, the attackers have indicated a desire for hacking not for political or monetary gain, but to bring to attention the issue of civil rights through attempting to "embarrass or discredit people". This is a credible website, because it has provided an author that stands behind the claims made, and a date that readers could cross reference with regarding the events discussed, along with references to their claims. It was published by Jenni Bengal on January 10, 2017 on a reliable website: http://www.pbs.org/newshour/rundown/hacktivists-launch-cyberattacks-local-state-governments/
    2. **Cyber Warfare**: In July of 2016, the Cymmetria cyber security company detected a cyberattack known as "Patchwork" and revealed that it had compromised around 2500 corporate and government agencies through code that was stolen from GitHub and the dark web. There were many victims of this attack, since it was not targeted towards one specific group alone. Specifically, the targets were focussed on those affiliated with military and political assignments in Southeast Asia, including governments and government related organizations. Because the attack was not detected immediately, and instead found after the damage had been done, the extent of the damage was able to increase. While the attackers are not known with certainty, it is believed that the attack is of Indian origin. These attackers exploited the Sandworm vulnerability, utilized a compiled AutoIt script, and a UAC bypass called UACME. Many infections on targeted

systems were initiated by spear phishing through emails that urged recipients to download a presentation that contained a the Sandworm vulnerability. The attacks also utilized different forms of second-stage malware. The attack was ultimately found since the attackers utilized technically simple attacks that were "amateurish" and did not attempt to avoid detection. To contain the damage of the attack, Cymmetria initiated an investigation to determine the extent of the damage. While it is unclear the motive of the attackers, it is likely that the operation was used to obtain sensitive information that could be damaging to the nations hacked. Since cyberwarfare is defined as the actions of a nation to infiltrate another nation's computer networks for the purpose of causing damage or disruption, this event is an example of cyberwarfare since many institutions suffered damages as a result of this attack. The website is credible since it contains an author (Tom Spring) and a date (July 7, 2016), as well as references to Cymmetria's website with a detailed report of the incident: https://threatpost.com/apt-group-patchwork-cuts-and-pastes-a-potent-attack/119081/

3. **Cyber Crime:** In 2012, there was a cyberattack against Wells Fargo that potentially compromised 70 million customers and 8.5 million active viewers. The attack was a denial of service attack that delayed and disrupted services on the customer website. Other banks such as Bank of America, Citigrouup, and PNC were all affected when customers could not access their online accounts. A group known as the Cyber Fighters of Izz ad-din Al Qassam claimed responsibility for the attack, and have stated that their actions were in protest to the anti-Islam videos posted on YouTube. The attackers used many different and complex tools that to pull off the attacks. The attacks were of a high "scale and speed", and have prompted U.S. Defense Secretary Leon Panetta to urge Congress and businesses to increase their cybersecurity efforts. Fortunately, the attack was detected quickly by Wells Fargo employees, and immediate action was taken to resolve the issue. Tim Sloan, the Chief Financial Officer of Wells Fargo has claimed that the bank continues to invest in its technology platform to defend against similar forms of attacks. These countermeasures in place were responsible for containing the extent of the attack, and minimizing the consequences on customer security. It appears that the attackers were motivated by a desire to impede operations of the banks to damage their reputation and prevent the peaceful conduct of business. This is an example of cyber crime, since it is characterized by a crime that involved a computer and a network. More specifically, there was an intention not only to discredit the banks, but also a desire to cause financial harm to the banks and their customers. This is a credible website, since it was published by a credible news source, and presents an author (Nicole Perlroth) and was reported when the event was recent (September 30, 2012): http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html
4. **Cyber Espionage:** In 2009, the Pentagon's $300 billion Joint Strike Fighter project was hacked by foreign spies. The Joint Strike Fighter, also known as the F-35 Lightning II, was the most expensive and technically complex programs that the Pentagon has ever approved. The hack by the intruders is clearly motivated by the objective to obtain sensitive information in foreign programs. According to former government officials, the attacks appeared to have originated in China. The intruders were able to obtain several terabytes of data relating to the design and electronics systems, making defense against the craft easier. The attackers were able to enter through vulnerabilities in the networks of contractors that were helping to build the fighter jet and encrypt the stolen data so investigators could not tell what had been stolen. While details such as the identify of the attackers and the scope of the damage to the U.S. defense program were never made

public, it is known that the most sensitive material stored offline was not compromised. According to Pentagon officials, the Pentagon systems are “probed daily” and is aggressively monitored for intrusion. Furthermore, appropriate procedures are in place to address these threats. Since foreign allies were aiding in the development of the aircraft, this opens up other avenues of attack for spies online. This is clearly an example of cyber espionage, since it involves obtaining secrets and information without the permission and knowledge of the holder of the information through computers. In this case, this was sensitive information belonging to a government agency that gave the attackers a military advantage. This is a reliable news source, since it was published by a well known company and featured several authors (Siobhan Gorman, August Cole, and Yochi Dreazen) along with updates, the last of which took place on April 21, 2009: https://www.wsj.com/articles/SB124027491029837401

3. Attack Tree to Access Investment Plan



In the attack tree, our goal to access the investment plan is represented at the root node. To accomplish this, we can either try to steal the laptop and then attempt to access the hard drive or password crack. However, this is not discrete, and may cause Jane’s company to change their investment plans. Alternatively, we can try to obtain access to the laptop. Since Jane has a busy travel schedule, one could attempt to wait for an opportunity when she leaves her laptop on in an unattended area. This may be time consuming, and there may not be an opportunity. We can also try to obtain access through social engineering, by exploiting the human attack surface. This could be accomplished through phishing through sending her an email pretending to be another entity, or by pharming through direction to a fake site. The other way to obtain access to the laptop would be to learn Jane’s password. Keylogging could be performed with hardware keyloggers to obtain the password. However, this may be difficult to accomplish and requires special equipment. The most direct approach would be to obtain the password from Jane. Some possibilities include threatening, bribing, and blackmailing her. These options do not appear to hold a high chance of success. Developing trust may be possible, but time consuming. Eavesdropping seems practical given these constraints.

4.

    1. We recall that entropy is log_2(N). A password consisting of only lowercase characters means that we have 26 options for each character. Since the password is of length 10, we have an entropy of log_2(26^10), which is around 47.00.
    2. A password consisting of lowercase and uppercase letters means we have 26*2 = 52 characters. Entropy is therefore equal to log_2(52^10), which is approximately 57.00.
    3. Passwords containing lowercase, uppercase, and digits, we now have an additional 10 possible characters. Entropy = log_2(62^10), which is around 59.54.
    4. With an additional 11 symbols added to the previous scenario, we now have 73 different possible characters. Thus, in our choice of 10 characters, each character can be any of these 73 possibilities. Entropy = log_2(73^10), or approximately 61.90.

5. In the following estimates, Tool 1 refers to https://apps.cygnius.net/passtest/, while Tool 2 refers to http://rumkin.com/tools/password/passchk.php.

Password	My Estimate	Tool 1 Estimate	Tool 2 Estimate
helloworld	47.00	14.874	36.4
HelloWorld	57.00	16.874	44.2
He110W0r1d	59.54	20.874	42.3
He!!0W0r1d	61.90	31.158	43.8

    1. According to our definition of entropy, as the password set size increases, the entropy of the password also increases. When a set S has N elements, the entropy of finding an element is log_2(N). Thus, when the set size N increases, entropy increases as well because log_2(N) increases as N increases. However, according to Tool 2, **HelloWorld** has greater entropy than either of the last two passwords that make use of a greater character set. This may be due to the method used by Tool 2 to estimate entropy, which estimates based on letter pair combinations in the English language. To make the frequency tables a reasonable size, Tool 2 was implemented such that all non-alphabetic characters were lumped together into the same group. For determining character sets in Tool 2, letters are grouped into a-z, A-Z, numbers, symbols above numbers, other symbols, and other characters.
    2. It is clear from the different results obtained between my estimate and those of Tool 1 and Tool 2 that tools for password strength estimation are just that - estimations. These tools can be used to give one a general sense of the password strength, but due to the different methods used for calculations and the different assumptions made about the means of attack, different entropy values are obtained. We can see that as my estimates

increase due to the increased character set considered, the other tools for password estimation generally show a similar increase (with the exception of **HelloWorld**), supporting the conclusion that these tools offer estimates that are correct relative to its own calculated value for various passwords, even though the estimates between tools may be different. Thus, tools for password strength estimation are useful in the sense that they can provide one with a good understanding of how strong their password is against different types of attacks. However, there is no guarantee that these entropy values are correct in all situations, since the attacker may utilize different forms of attack that the tools did not take into account. Furthermore, the results depend on the underlying datasets and algorithms that the tools use. It is ultimately up to the user to use the information provided by these password estimation tools to make an informed decision of whether they need a new password.

6.

1. Since a password consists of a string of 4 digits and we have 10 choices for each digit, we have 10^4 = 10000 different passwords.
2. h(7819) = (7^4+8^3+1^2+9)mod100 = (2923)mod100 = 23.
3. An example would be x = 0047, since (0^4+0^3+4^2+7)mod100 = (16+7)mod100 = 23
4. There are exactly 90 different passwords that have a hash value equal to h(7819). The code that I have used to arrive at this answer can be found below:

```
int count = 0;
for (int i = 0; i < 10; i++)
{
        for (int j = 0; j < 10; j++)
        {
                for (int k = 0; k < 10; k++)
                {
                        for (int l = 0; l < 10; l++)
                        {
                                int answer = (i*i*i*i+j*j*j+k*k+l)%100;
                                if (answer == 23)
                                {
                                        count += 1;
                                        //System.out.println(i + " " + j + " " + k + " " + l);
                                }
                        }
                }
        }
}
System.out.println(count);
```

5. We note that the probability of guessing John’s password when no hashing is involved would be 1 out of the total number of possible passwords that John could choose from. This is because without any additional information, the probability of correctly guessing the password cannot be improved, so brute force is required. Since there are 4 digits, with each digit taking any value from 0-9, we have 10^4 = 10000 different passwords. Thus, the probability of guessing John’s password when no having is involved would be **0.0001**. When hashing is involved, we note that in this specific case where the last

operation of the hash function is finding the remainder of integer division by 100, there are a total of 100 different hashed passwords (the values can be between 0 and 99 inclusive). Since this is the total number of possible hashed passwords, the attacker therefore has a 1/100 = **0.01** chance of guessing the correct hashed password. This is because any password that they choose to entered would be evaluated to 1 out of 100 different possibilities. It is clear that this is not a cryptographic hash function, which should be hard to invert (given a hash, it should be difficult to find the corresponding password), difficult to find two (x,y) such that h(x) = h(y), and should pass pseudorandom tests. Because the hash function used on John's password is not a cryptographic hash function, the hashed password does not offer a sufficient amount of protection.

6. In general, the purpose of using salt is to decrease the chance of success of an attacker who tries to guess a password. This is because salt, when concatenated with the password before being fed into the hash function, serves to increase the dictionary size that an attacker must precompute in order to successfully infiltrate the system. This is especially true when a large salt (32 or 64 bytes) is generated uniquely from a secure random number generator for each user. For instance, two users with the same password will now likely not have the same hashes, thus making offline dictionary attacks much more difficult. In our example however, we note that adding 2 digits of salt is not a large amount. Furthermore, any addition of salt does not change the fact that the last operation of this hash function is the mod 100 integer division. With the password of 7819, we can add any two digit salt to $7^4+8^3+1^2+9$. This could potentially change the hashed result from 23, since we are adding an arbitrary two digit value before finding the remainder when divided by 100. However, since we use the mod 100 of the result, this still leaves 100 different possibilities for the end hashed password. An attacker that is randomly guessing would still have a 1/100 chance of correctly guessing the correct hashed password. This reinforces the idea that while the principle of password salting increases the security against attacks, this must be used in conjunction with a good hash function (preferably slow and cryptographic based) to provide a noticeable advantage.