Computer Science COMP4670/8640

Assignment 1

Due: End of Friday, October 18, 2019

Note

Some questions might be open-ended and therefore require your own opinions and/or creativity, as the answers can vary considerably.

Question 1 (15%)

Based on the definitions we had for “Threats”, “Vulnerabilities”, and “Controls”, bring two separate examples or scenarios, and indicate each of these three aspects in each scenario.

1. It is the middle ages and a war has broken out between two factions (A and B). A message must be delivered from one kingdom in A to another, allied, country. This message details the plan that A will follow to attack B. A trusted messenger is told the message, replacing important parts with keywords, and sent on his way with a party of soldiers.

   Threats: The messenger may forget the message (Benign human error). Faction B may send somebody to stop the messenger from delivering the message.

   Vulnerabilities: The messenger is the single person (apart from whomever told him the message) who knows the details of the attack. Stopping or harming him would stop the information from reaching the allied country and cause the attack to fail.

   Controls: The messenger may be wearing armour to help prevent personal injury. Soldiers have been sent with the messenger to ensure his safety. The message was not written down so that the enemy cannot simply take the contents of the message. The important parts of the information were replaced with keywords so that even if the messenger were captured, the enemy still wouldn't know the exact details.

2. A hospital has a secured room devoted to research and development of a new drug. This drug is the first of its kind to be able to cure a certain disease, and other companies would like to get a hold of it so that they can either profit or copy the production method of the drug. To enter the room, one must scan their hospital-issued ID and their thumbprint. The time of entry and exit are logged. Cameras are watching the room.

After completion, submit your answers as a single pdf file into Blackboard.

Threats: There are people who want to either profit from or destroy this drug. A fire may break out in the room. A person may bring something out of the room with them.

Vulnerabilities: The room has one notable entrance: the door. Any building is susceptible to fire. Somebody could use someone else's ID to scan. Somebody could walk in with somebody who has access.

Controls: The door is locked by an ID scanner and additionally a fingerprint scanner. The time of entry and exit of the room are logged. Cameras watch the room at all times, allowing to see for certain who enters. An important room like that is likely to have a way to suppress a fire, either extinguishers or sprinklers.

Another possible answer:

Threat to a computing system is "a set of circumstances that has the potential to cause loss or harm", whereas **Vulnerability** is a "weakness in the system, that could be in the procedures, design, or implementation, that might be exploited to cause loss or harm", and **Control** is an action or measure taken to eliminate or reduce the vulnerabilities present in the system [1]. We can consider two examples:

Example 1: A major breach was discovered in

Molina Healthcare, a Medicaid and Affordable

Care Act insurer, that allowed its users to view the medical claims of other users by just changing a number in the URL address. In this case, the system did not ask for authentication before revealing the sensitive information. When this issue was bought into sight by security researcher, Brian Krebs, Molina Healthcare had to shut down their patient portals and improve the security requirement of the system [2].

In this case, the vulnerability in the system is that it does not ask for appropriate authentication in the system, when one authenticated user tries to access information about other users of the system (potential weakness in the system). The threat in the system is that when the user changes a number in the URL, the system gives access to sensitive information of other users without asking for further authentication (circumstance that cause loss to privacy). The control used here was that the system was shut down and appropriate measures

were taken to ensure proper access to authenticated users (action to eliminate the vulnerability).

Example 2: There was a major attack on Instagram, due to which the details of about 6 million of its users were exposed to hackers. The hackers exploited a bug present in the application's mobile API that gave out the sensitive information of its users. Further, Instagram removed the bug and the system does not pose the issue now [3].

In the above scenario, the vulnerability in the system is the bug that was present in the application's mobile API (weakness in the system) and the threat to the system is the potential attack of a hacker using the vulnerability, in this case, the bug, of the system (circumstance that cause loss to privacy). The control used here is that the bug was fixed and system made more secure (action to eliminate the vulnerability).

Question 2 (10%)

Using some sentences or examples, show how the four kinds of threats, "Interception", "Interruption", "Fabrication", and "Modifications" relate to the three concepts, preserving "Confidentiality", "Integrity", and "Availability". Is there a one-to-one correspondence between any pair of these concepts?

Interception

Interception is an attack against confidentiality. For example, WiFi Eavesdropping is one of the most common methods hackers use to compromise people private data. A hacker can obtain usernames and passwords of sessions connected to the free WiFi via snooping data. And if any bank transaction is made, the hackers will access the bank account information.

Other examples are packet sniffing and key logging to capture data from a computer system or network, or getting copies of messages to replay later.

Interruption

When an interruption attack happens, for example, a network service is made degraded or unavailable for legitimate use. These kind of attacks are against availability. DoS attack is an example of interruption where an overloaded service, bandwidth or system become unavailable.

Ping flood, SYN flood, and UDP flood are other examples that leads to the unavailability of the target system.

Fabrication

In this type of attack, a fake message is inserted into the network by an unauthorized user as if it is a valid user. This attack is against authentication, access control, and authorization but when attacker impersonate the valid user, it can result in the loss of confidentiality and integrity.

Modifications

In this type of attack, unauthorized modification (change, insertion, deletion) happens. It is an attack against:

- • Integrity: when a file is accessed in an unauthorized manner and the data altered, the integrity of the data is affected.
- • Availability: consider a configuration file that manages how a web service behaves, when contents of files are changed it might affect the availability of the service.
- • Confidentiality: suppose the configuration altered in the file for the web server is a part changes how the server deals with encrypted connections, it can be made as a confidentiality attack.

  There is no one-to-one correspondence between the type of attacks and the security services, because it depends on what the attacker is trying to achieve.

Another possible answer

Confidentiality:

Confidentiality is lost whenever an unauthorized agent gains access to assets. This corresponds to the threat of *interception*, that is, confidentiality is lost when an agent intercepts (gains unauthorized access to) assets on the wire or in storage. However, users can also be tricked into sending confidential information due to the *fabrication*

William Briguglio February 3rd, 2019 104 205 372

of fake certificates, the *modification* of DNS records, or by *interrupting* authentication

services.

Availability:

Availability is lost when an asset is not available to authorized parties at appropriate times. *Interruption* is related to availability in that interruption causes loss of availability when the threat is taken advantage of. Additionally, if a file is modified and the original contents is no longer available, then the threat of *modification* too, can cause loss of availability. Furthermore, we saw in scenario 2

how the *fabrication* of ARP packets can potentially lead to DoS. Additionally, although this is a contrived scenario, one can imagine that due to the *interception* of sensitive data, an organization which uses that data for authentication would have to discontinue their service since authentication is now unreliable. Thus, interception too can lead to loss of availability.

Integrity:

Integrity is lost when assets are modified (writing, changing, deleting or creating) by unauthorized agents. Obviously, *modification* and *fabrication* necessarily lead loss of integrity, but the threat *interruption* includes deleting a file, thus, in some cases interruption also leads to loss of integrity. Finally, Integrity is threatened when an unauthorized agent gains write access by *intercepting* authentication material.

Above, we can see that there is not a one-to-one correspondence between any pair of these concepts. Rather, the threats of interruption, interception, fabrication, and modification, can be used either alone or simultaneously to attack a system's integrity, confidentiality, or availability. In a summation, Interception, Interruption, Fabrication, and Modification, are all *threats* to Confidentiality, Integrity, and Availability.

Question 3 (10%)

Do you believe attempting to break into a computing system without authorization should be illegal? Why or why not? Bring at least two examples and/or scenarios to support your answer.

I believe the answer to the question "should attempting to break into a computing system without authorization be illegal" is more nuanced then a simple "yes" or "no". I think the unauthorized subversion of Integrity, Confidentiality, and Availability should be illegal without a doubt. However, I believe, and I think most security analysts agree in some way, that the best test of a cryptosystem or security system is the "test of time". That is, I think that allowing white-hat hackers to attempt to break into a system to discover bugs and points of weakness not only helps the production of more secure systems, but also helps individuals and small corporations who cannot afford pen-testing to maintain their security. In support of this, I site this article, https://www.dailymail.co.uk/news/article-6514443/White-hat- hacker-talks-directly-man-Nest-camera.html, where a homeowner was alerted that his security camera was compromised by a white hat hacker. To clarify, I believe hackers with appropriate government licenses and with standardized methods endorsed by the government and developed by security specialist should be allowed to use threats of interruption, interception, modification, and fabrication to illustrate to users how their system is insecure, without actually stealing, modifying, or denying access to any sensitive data or denying access to sensitive services.

Another possible answer:

Attempting to break into the system should be illegal in my opinion. However, there should be layer of punishment according to the type of the hack/hackers. Since most of the computer crimes are done by the amateurs due to their curiosity, the idea of giving them the highest level of

punishment as a lesson to all the hackers (e.g. Career Criminals or Terrorists) might bounce back with a negative impact in the "ethical hacking" industry. Since the job of ethical hackers is to find out the holes in the system, this might motivate them to lose their interest in this sector which will slow down the development of the overall security system.

Example 1: Where the attacker should be dealt with a serious level of punishment
Marriott International, in November 2018, declared a cyber-attack in their system. The attackers remained in the system after Marriott acquired Starwood in 2016 and were not discovered until September 2018. About 500 million of people were victimized of the attack.
Later on it was found that a group of Chinese intelligence were responsible for the attack where their main goal was to collect the information of the US citizen.
Example 2: Where a serious punishment could bring a negative impact in the overall development of the system's security
Joanna Rutkowska, a famous white hat hacker, exposed her hacking capabilities in 2006 while presenting at the Black Hat Briefings conference. There she demonstrated the vulnerabilities in Vista kernel.
Later on she became the founder of the desktop operating system Qubes OS, a security focused operating system.

Question 4 (15%)

For each of the following two programs, answer the three questions followed:

1. A program that accepts and tabulates votes in an election.
2. A program that allows consumers to order products from the web.

- Who might want to attack the program?
- What type of harms might they want to cause?
- What kinds of vulnerabilities might they exploit to cause harm?

A program that accepts and tabulates votes in an election.

• Who might want to attack the program?

➔ The attacker might be paid by any particular party who took part in that election and now tries to deviate the result of the election towards their favor.

• What type of harms might they want to cause?

➔ The main goal of the attack is to change the result of the election in favor of a particular decision/party/opinion. This will eventually abolish the main motto of any election (to select a particular decision/party/opinion fairly and without being biased).

• What kinds of vulnerabilities might they exploit to cause harm?

➔ The attacker can exploit any type of vulnerabilities to damage the cause of the election. They might try to steal the data storage where all the data kept, might come up with DOS attack, might get into the network to intercept or modified the data or might come up with a method which will not allow the legit voter to get into the system to cast their vote.

A program that allows consumers to order products from the web.

• Who might want to attack the program?

➔ Any person with required skillsets and whom has the interest about the products or want to get the personal information of the user might attack the program.

• What type of harms might they want to cause?

➔ These attack can cause damage from personal level up to corporation. If they somehow able to steal the personal information of the user they can

- use the user credit card
- analyze the shopping pattern of the user and use the card accordingly
- Identify user's lifestyle and make a clone of user's identity and can use it in criminal

activities
- Sell the user's personal information in the black market
- Blackmail the user with their sensitive information

These will eventually destroy the brand value of the corporation which might lead them to a million dollar loss.

• What kinds of vulnerabilities might they exploit to cause harm?

➔ To me the most vulnerable part for these kind of attack is the network of the system. If the browsing network (since it is an online shop) or payment channel of the system is not strong enough, the attacker can deviate the customer's attention by sending him/her a lucrative offer (which is basically a malware or spam) and eventually get their credit card's information. The attacker even might attack the system disguising him/herself in the customer's "uniform".

Another possible answer:

Program 1: A program that accepts and tabulates votes in an election
i: This program could be targeted by anyone with the goal of subverting the democratic process.

Parties themselves may be trying to fraudulently win extra votes however foreign governments may also see value in manipulating votes (see Russia in the 2016 United States Presidential Election) or just anyone with the goal of disrupting government processes. E.g.) In the Comodo Threat Research Labs Global Malware Report for 2017[1], they reported a massive increase in malware infections during the time approaching the U.S. Election.

ii: The harm these attackers might cause is in the removal, modification, or fabrication of votes in the case of someone trying to sway the election results. Additionally, the voting process is meant to be confidential for the safety of voters, however a party could attempt to steal voter names and target individuals with strong man intimidation techniques. Finally, people who despise the government or who take joy in disrupting other people's work, may try to take voting machines offline. Across these cases we see an attack on Confidentiality, Integrity, and Accessibility.

iii: In this situation, attackers may try to exploit vulnerabilities in the communication protocols used by the machines to send voting results or take advantage of any lack of physical security such as uncovered USB ports or input devices that respond to secret inputs to grant different privileges. They could also take advantage of any remote database/server used by the program. Also, if they only wish to disrupt the voting process, they could attack the machines power supply either directly or indirectly.

Program 2: A program that allows consumers to order products from the web
i: Multiple agents could see value in attacking this program. The obvious examples are anyone trying to make money by selling personal data or using banking data illegally. Additionally, advertisers may be after your purchasing information in order to create more effective adds. Even if they do not engage in cyber-attacks directly, they may offer money for this information and thus create incentive for cyber criminals to attack this program.

ii: Once data on purchasing history is obtained, attackers may sell this data to advertisers, use this data to create personalized phishing emails, or blackmail users if the purchasing history is something they wish to keep private. If User's passwords, emails, or account recovery questions are stolen, attackers can use this data to access a user's account on this program or access other accounts that uses the same passwords, emails, or recovery questions. If banking information is stolen, attackers can use this data to make fraudulent charges to the users' credit cards.

iii: In this situation, the attack vectors are numerous. The program itself could have bugs in its implementation that allow attackers to infer passwords from hashes or see plain text passwords. The communication protocols might not securely encrypt data as it travels over the wire. The database user data is stored in could have vulnerabilities in the way data is accessed or stored. Any incoming communications can have code injections or alterations that cause the program to behave in unexpected ways. If input strings are not sanitised, then the program or the database serving the program could be vulnerable to injection attacks. Leftover testing functions could give too much power to users with malicious intent. Due to the wide appeal of the data that is handled by this program, virtually every aspect of it could be attacked, and even the program itself could serve as an attack vector for a larger attack. For example, if the program demands unnecessary privileges form the OS it runs on, then attackers can use this for Privilege Escalation to perform other attacks on a user's machine.

Question 5 (10%)

After completion, submit your answers as a single pdf file into Blackboard.

One-time Pad is the only cryptosystem that provides ***Perfect Secrecy***.

- Describe advantages and disadvantages of this cryptosystem.
- Advantage: with Perfect Secrecy, given a ciphertext, every message in the message space is exactly as likely to be the underlying plaintext. So, the plaintext is independent from the ciphertext. Thus the perfect secrecy requirement implies that the eavesdropper truly learns nothing at all about the underlying plaintext.
- Disadvantage: It is impractical, because for every plaintext we need a truly random key to apply, so secure key distribution is an obstacle. We also need a key with the same length as the plaintext.

Advantages	Disadvantages
i) Cipher text provides no additional information about plain text. ii) Encryption and Decryption are the same operation and Bitwise XOR is easy to compute. iii) It is as secure as theoretically possible (if key sequence is truly random).	i) Unlimited number of keys is required. Although generating such keys is possible, the distribution and storage of such keys are the main problems. ii) Sender and Receiver must be synchronized. iii) The length of key can be very large if the plaintext is very large as key must be as long as the plain text. iv) It does not ensure Integrity that is attacker can modify the plain text easily.

- Bring one example in real-word, in which one-time pad is suitable to be used, and one example that is not. Justify your answers.

  Suitable for one time password and session key.

  Not suitable for very long messages.

Example-1: One time pad can be used for secret short message communications between two embassies by fulfilling some conditions. Like, the pad must be exchanged secretly and both parties must be synchronized. Moreover, there must be some limit on the length of plaintext. That is message must be broken into to be fit into the limit. As a result the key distribution and storage will be manageable.

Example-2: One time pad is not suitable for encrypting very large plaintext generated from an environment monitoring satellite. That is the data can be potentially infinite in length. As a result the length of key will be also potentially infinite. This will cause problem for the key management.

Question 6 (10%)

After completion, submit your answers as a single pdf file into Blackboard.

Rotor machines were used by both Germany (Enigma) and Japan (Purple) in World War II. Watch this short clip on Enigma rotor machine:

http://www.khanacademy.org/math/applied-math/cryptography/crypt/v/case-study--ww2-encryption-machines

It consists of a set of independently rotating cylinders, each of which has 26 input pins and 26 output pins. Each input pin is connected to a unique output pin using internal wiring. You can see a related diagram in the following link, under the title "Rotor Machine":

http://sjsu.rudyrucker.com/~haile.eyob/paper/#3.%20Classic%20Cryptography

- A single cylinder defines a mono-alphabetic substitution. Considering a 5-rotor machine, what would be the equivalent key length of a Vigenere cipher for this machine? Explain your answer.

A 5-rotor machine uses 26^5 different substitution alphabets before the system repeats. In a Vigenere cipher the length of the key determines when the substitution alphabet repeats, so we need a key of length 26^5.

- Humans are said to be the weakest link in any security system. Give two examples of human failure that could lead to compromise of encrypted data.

(a) Choosing weak passwords of simple and short words which are easy to guess, and using the same password for all devices or using a password for a very long time

(b) Clicking on malicious web links; due to curiosity and ignorance

(c) Data breaches in companies caused by employees who use their personal laptops, USB and mobile phone to access organizational data and then carrying these sensitive data on their personal computers

(d) Accessing internet via insecure wireless connections

After completion, submit your answers as a single pdf file into Blackboard.

Question 7 (5%)

Based on the convention we use to represent English alphabet using numbers 0 to 25, try to formulate Atbash Cipher by showing two mathematical expressions, one for encryption and one for decryption. Show the correctness of your expressions with one example.

Question 8 (15%)

Affine Caesar cipher is a generalization of the Caesar cipher, with the following form:

$$C = E([a,b],p) = (ap + b) \bmod 26$$

- What would be the limitations for the possible values of *a* and *b*? Explain why. Provide your answer as a general statement.

In Affine Caesar cipher, the value of "a" will be relatively prime to 26 (as there are 26 letters in English alphabet). That is, "b" will be an integer between 0-25.

The possible twelve values of "a" will be 1,3,5,7,9,11,15,17,19,21,23,25. So,

- Based on your answer to the first part of this question, how many distinct affine Caesar cipher exist? Explain your answer.

  Number of distinct Affine Cipher= 12*26 = 312.

- The following ciphertext has been generated with an affine Caesar cipher. Break the code. **(It is important to show all the cryptanalysis steps you perform, and not just writing the final answer.)**

  rarxl jobfp lobvb egler jnoob jgbej ozwgl

  nelxg crglg xcnpm sabne bgnne b

  Hint:

  First indicate the first two most frequent letters in the cipher.

  a = 9, b = 17

  a basic requirement in a correct encryption is that it should be one to one

After completion, submit your answers as a single pdf file into Blackboard.

Question 9 (10%)

- How would you test a piece of ciphertext to determine quickly if it was likely the result of a simple substitution?

Calculate the frequencies of all letters.
Match the frequency of every letter with the frequency of letters in English letters.
By performing a frequency analysis and counting the number of letters, digraphs and trigraphs we can find out whether the cipher text bears any statistical relation to the natural language. If it is the result of a simple substitution then the frequency should be similar to natural language but with different alphabet.

- How would you test a piece of ciphertext to determine quickly if it was likely the result of a transposition?

If the cipher is result of a transposition, then the number of occurrences of a specific letter in plain text cannot change in the cipher. So the frequency of letters should be exactly that of natural language.

After completion, submit your answers as a single pdf file into Blackboard.