

Name:

Information Assurance: Homework 2 Answers and Comments

Due September 12, 2007 on compass.

1. Consider online credit card transactions. Describe an example of each of the following: (15 pts)

There was some confusions about the distinctions between these three concepts. There are many options for answers. Here is one set.

- a. A security requirement

Exposure of sensitive customer information must be minimized.

- b. A security constraint.

All credit card information must be kept confidential as it passes over the network.

- c. A security control.

A TLS/SSL tunnel using AES 256 encryption between the client and the vendor and between the vendor and the credit card company.

2. A team of experts using the quantitative risk analysis approach has reviewed a software development organization. They identified the two most important assets of the organization, the value of each asset, and the probability that a threat would be successfully launched against each asset of a 12 month period. (29 pts)

Asset	Value	Risk over a year
Product Source	\$1,000,000	1%
Customer Records	\$250,000	10%

- a. What is the risk exposure/annual loss expectancy for each asset? (4pts)

Product source risk exposure = \$10,000

Customer records risk exposure = \$25,000

- b. The experts have identified two control options

Control	Cost	New Risk for Source	New Risk for Records
Wonder Security Product	\$100,000	0.5%	1%
Hire Security Officer to Improve Implementation of Existing Controls	\$200,000	0.1%	5%

Name:

Calculate the Risk Leverage in both cases. Based on the Risk Leverage numbers, which control would you recommend trying first. (5 pts)

Risk Leverage = (Risk Exposure before control – Risk Exposure after control)/cost of control

Wonder Security RL = (\$10,000 + \$25,000 - \$5,000 - \$2,500)/\$100,000 = 0.275

Security Officer RL = (\$10,000 + \$25,000 - \$1,000 - \$12,500)/\$200,000 = 0.1075

Based on the risk leverage calculation, I'd go with the Wonder Security Product.

Some people computed the risk leverages for the assets separately. You did not lose points for that, but by combining the assets you get a single number and you have an easier task in the comparison.

c. Identify two additional assets of the organization (4pts)

There are many possible different assets for a software development organization. Some assets include:

- *Building*
- *Computers*
- *Cash on hand*
- *Employees*
- *Intellectual property, e.g. Patents, designs, etc.*
- *Plans for future products*

d. Identify three potential threat sources. Use the MOM (method, opportunity, motive) technique to characterize the threat sources. (10pts)

There are many possible threat sources. Here are three examples.

Competitor:

Method: Understands the business, so knows how to work in the organization. Software savvy. Has some monetary resources.

Opportunity: External access. If he can social engineer his way in, he might have some inside access. Competitor is likely willing to commit some time and effort to the attack.

Motive: Beating the company in the marketplace

Cleaning staff:

Method: Limited technical skills but may know where things lie physically

Opportunity: Has full physical access

Name:

Motive: Monetary gain.

Organized crime

Method: Could hire very technically skilled people

Opportunity: External access. May be able to bribe to gain internal access.

Motive: Depends on the type of software being developed. May just want to extort money from company by threatening denial of service attack or revealing unpleasant facts about the company to their customers.

Some people mentioned natural disasters, e.g., earthquake or fires. This is quite a legitimate threat source though not a intelligent malicious source. Ascribing motive to a natural disaster is a bit tricky though.

- e. For each threat source identify the asset of greatest interest. (6pts)

Competitor: Product source, future plans, and customer records

Items they can use to gain a competitive advantage against the company.

Cleaning staff: Computers, cash on hand

Items that can be easily converted to cash.

Organized crime: customer records, computers, cash on hand

Items that can be easily converted to cash or information that can be used against the company.

3. Cipher texts resulting from substitution and transposition ciphers have different characteristics. Identify the most likely class of cipher in each case below: (10pts)

Many people had problems with this question. Most people who got this wrong provided no reasoning on their answers, so we could not assign partial credit.

- a. Characters in the message have a statistical distribution close to that of standard English messages

Transposition. Since the characters have not been changed, the statistical distribution of the characters (not shifts or other variants of the characters) should match those of standard English for a large enough English message.

- b. Digrams in the message follow the same statistical frequencies as those found in standard English.

Potentially substitution. However, in this case, the digrams will be shifted. So instead of "th" the digram might be "xz". In the case of a simple substitution for a long enough message, the pair "xz" will show similar frequency to "th" in the English average. For a transposition, it is unlikely that the digrams (adjacent characters) will bear any relation to the average frequencies of digrams in English. Similarly, more complex substitutions that have varying character mapping (e.g. One time pads and Enigma) will also be unlikely to show common digram frequencies.

Name:

4. The message below is encoded using a book code with the course syllabus page as the key <http://www.cs.uiuc.edu/class/fa07/cs461/syllabus.html>. Decode the message. (10 pts)

VVVYTONLDEIZSFWGHVALWNCFPZHVL

You should have used the text from the syllabus page for the book cipher key. This should have generated the following plaintext

Congratulations today is your dax

The last word should have been day, but I made an error while fixing a last minute detected typo.

5. Determine the key and decode the vigenere encrypted text assigned to you in compass. You may use automated tools such as the applet discussed in class <http://math.ucsd.edu/~crypto/java/EARLYCIPHERS/Vigenere.html>. (14pts)

The plaintexts will be posted on the web site. Most people got this correct. Some people forgot to add the key and lost a few points on that.

6. Encode the following message using columnar transpositions. Use Z as a pad character as necessary (10pts)

Tw as brillig, and the slithy toves
Did gyre and gimble in the wabe:
All mimsy were the borogoves,
And the mome raths outgrabe.

- a. Encode using a 2-columnar transposition (also known as a rail transposition).

TABILGNTELTYOEDDYENGLMITEAELMMYEEHBRGVSNTTEOEAHOTRB
WSRLIADHSIHTVSIGRADIBENHWBALISWRTEOOOEADHMMRTSUGAE

- b. Encode using a 7-columnar transposition.

TLTHDALWMRRAOSB
WLHYINEAIEONMOE
AIETDDIBMTGDEUZ
SGSOGGNESHOTRTZ
BALVYITAYEVHAGZ
RNIERMHLWBEEETRZ
IDTSEBELEOSMHAZ

7. One time pads are “perfect” ciphers if the keys never predictably cycle. If the key stream is random so is the ciphertext. However, if the key stream repeats, the interceptor can get two streams of ciphertext that use the same key sequence. He can use these two ciphertext streams to get a text sequence that is only a function of the plaintext (the keys are canceled out).

Name:

In substitution cases discussed in the book, the encryption algorithm is $E(p_i, k_i) = (p_i + k_i) \bmod 26$. Assume you are given two ciphertext sequences X and Y that are results of encrypting different plaintext with the same keys. Show how X and Y can be combined to create a function that is only a function of the plaintext of X and Y. (12 pts)

This idea here is that by subtracting the ciphertext strings, you will cancel out the keys. You can show this by substituting the encryption clause for the cipher result as shown below.

$$E(x, k) = (x + k) \bmod 26 = X$$

$$E(y, k) = (y + k) \bmod 26 = Y$$

Say $X > Y$

$$X - Y = (x + k) \bmod 26 - (y + k) \bmod 26$$

$$= x + k + c1*26 - (y + k + c2*26)$$

$$= x + k + c1*26 - y - k - c2*26$$

$$= x - y + (c1 - c2)*26$$

$$X - Y = x - y \bmod 26$$

While you aren't directly solving for a single plaintext, the resulting combination of two plaintext streams will still have similar characteristics to the original language. One of you pointed out that the combination will have similar characteristics to a book cipher ciphertext.