Approaching and Answering In-Depth Exam Questions

Jacob Löfvenberg
Department of Electrical Engineering
Linköpings universitet
jacob@isy.liu.se

John Wilander
Department of Computer and Information Science
Linköpings universitet
johwi@ida.liu.se

January 10, 2006

Read the directions and directly you will be directed in the right direction.

The Doorknob, Walt Disney's Alice in Wonderland, 1951.

1 Introduction

Sometimes as a teacher, when you correct the exam of a student, you get the feeling that the student has not achieved as well as he or she could have done – not because the student did not know the subject, but because of how he or she addressed the question and wrote the answer. This paper is a way for us, as teachers, to try to explain what it is we expect students to do when addressing in-depth exam questions, and we do this by describing a model of how to work with exam questions and by giving tips on how to formulate answers.

It is important to understand that this is meant as a guide, helping students who may have problems coping with the exams otherwise. It is not the only way to address exam questions, and it is not a requirement to follow the model. Our goal with this paper is to avoid students getting lower grades than their knowledge allows.

The paper is divided into two parts: the first discussing how to approach in-depth questions, and the second discussing how to formulate answers.

1.1 Addressing In-Depth Questions – A Structured Approach

First, we need a structured way of approaching in-depth questions. The goal is to break the question down into the parts that ask for an answer. This means dividing the question into what we call *deliverables*. Second, we brainstorm and connect the question to our knowledge-base. Finally, we formulate an answer covering all the deliverables. Step-by-step the structured approach looks like this:

1. Analyze the question
   - Keep in mind the course context and try to have that perspective when reading the question.
   - Underline all parts of the question that explicitly ask for an answer. This means dividing the question into deliverables.
   - Make a check list of the deliverables. This list will be used to ensure that all parts of the question have been answered.

2. Process your knowledge
   - Ask yourself "What do I know about this?". Brainstorm and take brief notes of what you come up with.
   - Try to combine and find connections between the various pieces of knowledge you possess. This is the very essence of showing what you have learned and that you can discuss the material (see figure 1).

3. Conclude and Answer
   - Show your knowledge and draw conclusions of your own. Since it is an in-depth question the answer is not only what you know by heart.
   - Write readable, structured, and clear answers.

- Justify your statements and avoid too strong statements.
- Use the check list you developed during the analysis of the question.
- Make use of examples. This often helps to show your knowledge and understanding.

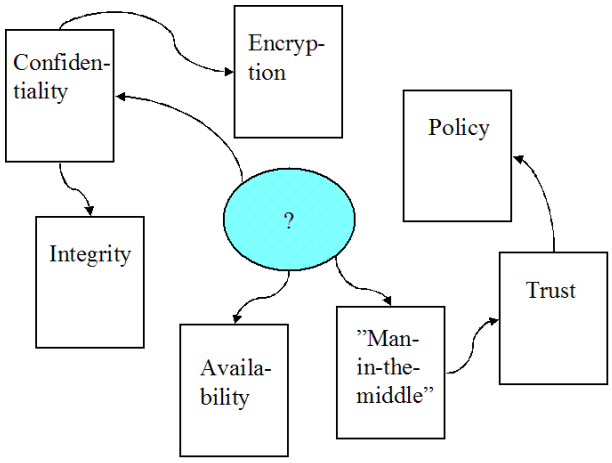

Figure 1: Visualization of processing of knowledge. The picture tries to show how knowledge can be combined and connected to draw conclusions and show in-depth understanding. Boxes visualize pieces of knowledge and arrows connect the knowledge to the question and to other pieces of knowledge.

2 Example: In-Depth Question on Secure Networks

The following is an example of what the process of analyzing the question and processing our knowledge could look like for a realistic question on secure computer networks:

> **In-Depth question on Network Security:** Computer networks can be both wired and wireless. Compare wired and wireless networks from a security point of view. Describe and motivate significant differences. Give an example of an relevant attack form possible in both wired and wireless networks and highlight differences both from the attacker's and the defender's point of view.

First, underline the deliverables in the question:

> **In-Depth Question on Network Security:** Computer networks can be both wired and wireless. Compare wired and wireless networks from a security point of view. Describe and motivate significant differences. Give an example of an relevant attack form possible in both wired and wireless networks and highlight differences both from the attacker's and the defender's point of view.

Then produce a check list covering all the underlined parts of the question:

- Compare wired and wireless
- Describe and motivate differences
- Example of attack form possible in wired and wireless
- Highlight differences from attacker's point of view
- Highlight differences from defender's point of view

Now it is time to look into our inventory of knowledge, which we assume to be that obtainable by following any basic security course.

We start by asking ourselves what we know about analyzing security? Some basic categories might help so we start with the *CIA model*, dividing security into Confidentiality, Integrity, and Availability. What are the differences in C, I, and A between wired and wireless networks?

Confidentiality. To have the same level of confidentiality in both kind of networks we will need some kind of encryption in the wireless case.

Integrity. Wireless networks might have more erroneous traffic so there might be need for error-checking or error correcting codes. How do they affect security? Any special attacks possible by fooling the error correction?

Availability. The possibility of re-routing traffic in wireless networks allows for defense against certain availability attacks (compromised node can be frozen out). What about denial of service?

This was to show how we can discuss with ourselves and generate in-depth answers to quite open questions by brain storming and taking notes (even of thoughts and ideas). From this process we should be able to formulate a satisfying answer to the first two parts of the check list.

We then move on to process possible attack forms and highlight differences from both the attacker's and the defender's point of view.

An example of a relevant attack form possible in both kind of networks is the so called *man-in-the-middle attack*, also part of basic security. The attacker tries to hijack a connection between two peers by faking his or her identity and staying in-between the two peers.

1. Man-in-the-middle from an attacker's point of view
    - In a wired network the attack is hard to initiate since you have to cut the wires or get access to a router or the like.

- In a wireless network the attack is easy to initiate since you just tap in. You may not even have to be in the same building.

2. Man-in-the-middle from an defender's point of view
   - In a wired network the defender will have a hard time detecting the attacker on the network since the lost connection to the peer might not be detectable.
   - On the contrary, in a wired network it will be easier to find an attacker or attacking entity *physically*—you just check the wires.
   - In a wireless network the defender will have an easier task to detect the attacker on the network since it might be possible to hear traffic from both the peer and the attacker at the same time.
   - But in a wireless network it will be harder to find an attacker physically since there are no wires to follow and the attacker node might be mobile.

What we have done so far can be visualized as in Figure 1. There are several parts, but the different parts are connected in some way. Thus, we have the knowledge, and we know the structure. What is left to do now is formulating the answer.

3 How To Formulate an Answer

In this section we address some issues regarding how to formulate a satisfying answer. First some important areas which can cause problems are described, and after that examples are given of how to, and how not to formulate answers.

- Write readable answers
- Write structured answers
- Write clear answers
- Avoid strong statements
- Justify your statements
- Give a complete answer
- Make use of examples

3.1 Topics in Formulating Answers

3.1.1 Write Structured Answers

Structure your answers and write coherently. Your text should always be a coherent whole, and not split into parts without obvious relation. If your line of thought is not visible in your answer, the person correcting the exam may think that your grasp of the subject is lacking. You may find it useful making a clean copy of the answer (rewriting it) when you are done with a question. That way you can make adjustments in layout, formulations and handwriting when you know what you want to say.

3.1.2 Write clear answers

Be as clear as possible when saying something. Vague or unclear statements makes it difficult for the person correcting the exam to form an opinion of your knowledge.

3.1.3 Avoid strong statements

Do not make stronger statements than you can motivate. Most things have both strong and weak sides. In such cases, saying that technology XX is "the best solution and has no problems" is not a good idea (such statements are seldom true). Instead, if you want to say something about XX, say for example that "XX is often used, since it does not suffer from weakness YY. On the other hand XX can not handle ZZ, so when ZZ is needed you have to use something else".

3.1.4 Justify your statements

If you make a statement about something that is not a clear fact, you should justify the statement (that a statement is taken from a book does not automatically make it into a fact). You should not say: "if compact implementation is needed XX can be used", but instead "if compact implementation is needed XX can be used, since its use of the splurification transform makes it much smaller than table look up techniques".

3.1.5 Give a complete answer

Make sure that you answer the question. After writing your answer it is a good idea to reread the question to ensure that you have understood the question correctly and that your answer matches the question (here you can make use of your check list). Remember that, especially for in-depth questions, a long elaborate answer may be needed to get a good score, even if a single "yes" or "no" (technically) answers the question.

3.1.6 Make use of examples

When describing something it is often a good idea to give an example. We did so in section 3.1.3 on avoiding strong statements. Our hope is that the "abstract" description will be easier to understand when there is a simple example.

3.2 Examples of Formulations

All the numbered examples in this section relates to the enlisted tips in the previous section.

3.2.1 Example on Writing Structured Answers

Don't write
Wireless networks connect nodes without using wires. Encryption can be used for privacy. Radio signals can be received from a long distance.
Instead write
Wireless networks connect physically separated nodes by using radio communication instead of wires. From a security point of view, a problem with such a solution is that radio signals can be overheard from long distances, and thus such signaling is not secure unless protected by encryption.

3.2.2 Example on Writing Clear Answers

Don't write

1. Man-in-the-middle attacks is used between Alice and Bob.
2. Encryption is used to make information unreadable.

Instead write

1. A man-in-the-middle attack is an attack where the adversary inserts himself between the two communicating parties (Alice and Bob) without them knowing it. Alice and Bob communicates with the attacker, but think they are communicating with each other. In this way the attacker not only learns everything from the communication, but this kind of attack also defeats some cryptographic protocols, for example Diffie-Hellman key exchange.
2. Encryption can be used to make information unreadable to everybody not having the correct key.

3.2.3 Example on Avoiding Strong Statements

Don't write

1. Encryption solves the information security problem.
2. Using wired networks there is no possibility for eavesdropping.

Instead write

1. Encryption can be used to address several different security problems, and is an essential part in a secure communication system.
2. Using wired networks makes it necessary for an eavesdropper to physically visit the network he wants to attack, which can be made difficult in some cases.

3.2.4 Example on Justifying your Statements

Don't write

1. Wired networks are more secure than wireless networks.
2. The DES cryptographic algorithm is not secure.

Instead write

1. Using wired local networks makes it necessary for an attacker to physically visit the network he wants to attack. In such cases, if the physical security is good, then wired networks are advantageous.
2. The DES cryptographic algorithm uses a key of only 56 bits. With modern electronics 56 bits is possible to successfully attack by brute force, thus making DES to weak for secure applications.

4 Improvements of this Document

Having read this paper to its conclusion you may feel that something is missing or that something should be improved or changed. Another section, on some related topic could perhaps make the document much better?

If you have this feeling, and especially if you have explicit ideas of how to improve the text, please contact the authors or the managers of the course in which you received the document.