STIMULATING STUDY OF COMPUTER SECURITY

Anatoliy Gordonov
anatoliy.gordonov@csi.cuny.edu
College of Staten Island
2800 Victory Blvd., SI, NY 10314

Abstract: Security is a complex problem. It includes many aspects, such as physical security, network security, operating systems security, database security, WEB and Internet security, software (SW) development security, users' security, and more. The success of any security policy heavily depends on the human factor. In this paper we have considered the emerging problem of security education: how to motivate the students to learn computer security. We surveyed different groups of students including students with computer science and non-computer science majors. The results of this survey are presented and analyzed separately for the networks and software related vulnerabilities and threats. Our research shows that many students (both with computer science and non - computer science majors) are unaware of security problems and threats and, therefore, need additional motivation to study security. Examples of the author's experience in teaching security courses are presented. The results of the research may be useful for those who are planning to develop new security courses or introduce a richer security component in the existing courses.

Key words: Computer security, human factor, security education, motivation.

Introduction

The success of any security policy heavily depends on the human factor. In other words, no system can have a high level of security if people who develop, install, and use it do not understand what problems insecure use can cause. The answer seems to be very simple: teach those who deal with computers proper rules of security, and this will solve many problems. Unfortunately, it is not always true.

Many of the security rules are very simple: select the right password, do not leave your password in a place where other people can easily see it, do not leave your computer unattended and running. Among other rules we can mention are the following: do not read suspicious e-mails, always check the length of the input information in your program, and many other simple or relatively simple rules that have to be adhered to. Many users and developers are familiar with these rules, but we can still see that breaking them is the reason for security problems.

Stimulating Security

The name of this paper:" Stimulating Study of Computer Security" may sound strange. Who wants to work in an insecure environment? Let us teach students how to work securely with computer systems, and this would solve the problem. Unfortunately, this is not a complete solution.

If we try to plant a flower in the soil that is not prepared specifically for it, the flower fades out after a while. In order to study and then use security rules, students have to be prepared for this. They have to fully understand the consequences of breaking these rules.

Here I would like to give an example for the security and privacy motivation, which I used at the very beginning of my "hacking" course. This course is taught at the time when students have already taken the first programming course but have not learned anything in security so far. The scenario is very simple. Before the beginning of the first class, I ask somebody (a person who is not known to the students) to come to the class and announce that the professor will come a little later, but he asked the students to answer a short questionnaire. The questions include general information about students (such as name, number of credits taken so far, Grade Point Average …) and also information about computers, operating systems, and applications they are using. The questionnaire is short, and it takes just about 3 minutes to fill it in. After this, my assistant collects the data and leaves the class. I am entering the classroom immediately apologizing for the delay. Typically, someone from the class asks me something about the questionnaire (for example: "Professor, did you get our answers?"). Now it is my turn to act. I am making a surprising face and say that I do not know anything about the questionnaire they are talking about. When I learn that my students gave their personal information to an unknown person, I tell them that now they can expect to have many problems. I have played this scenario several times with some variations, and every time my students have remained silent and shocked. At this moment the students begin to realize that they have done something wrong. Of course, I explain to them that this is just an example of what may happen in the real world. But I believe that this is "a moment of truth" for many of my students, and they start understanding that security is something very real.

Learning from the Students

There is nothing more useless and unproductive than trying to encourage people to do something if they are already motivated to do this. So we decided to learn how many of our students are motivated to study security. Motivations are definitely related to the level of awareness about security threats. We have carried out a research focused on how our students understand various security problems. Thus, we anonymously surveyed the students giving them a number of questions about various security problems.

Before describing the results, let us give the structure of the questionnaire used, numbers and characteristics of the students who participated, and the way we analyzed the students' answers.

Altogether about 150 students participated in this survey. We separated them into three categories:

1. Students who are not computer science (CS) majors and have some computer experience at the users' level. These are non-science students who took an elective general education course "Introduction to Computer Technology". 18% of the students participating in our study fall into this category.
2. Students who are CS majors and have some programming experience (have taken at least one programming course). This category includes 18% of all students.
3. Students who are CS majors have taken at least one programming course, and studied at least one course in computer security (64%).

The survey includes the following types of questions:

1. Related to network security (40%);
2. Related to programming security (30%);
3. Related to operating systems security (20%);
4. Related to database security (10%).

In our analysis we are going to focus on the first two types of questions.

The answers that students had to give were not multiple choices. Instead, they had to write several sentences or say "I do not know". For the convenience of our analysis, we divided all the answers into the following groups:

1. *"I do not know"* group. These are the answers in which students explicitly or implicitly showed that they did not have any idea about the question asked.
2. *"Have an idea"* group. These students displayed the understanding of the existence of a problem.
3. "*Have some specific knowledge"* group. Students in this group showed more extensive knowledge about a problem including ways of resolving this problem.

We are going to analyze the students' answers for two major categories of questions: networks and programming security. The survey results are shown in figures 1 and 2.

As we could expect, non-CS students have much less understanding of security threats and, therefore, less motivation to study them.

We observed a similar, but not so explicit, tendency for students with CS majors who already studied programming but did not take any security related courses. We received better results for the students with CS majors who already studied security courses.

All the results mentioned above are obvious. A more detailed analysis shows that 22% of CS students answer "I don't know" to a question like "Why do you think networks are vulnerable to the attacks?", and 25% of these students answer that they do not know anything about security problems in programming (one of the question in this group was:"What kind of program flaws do you know that can cause security threats?"). In other words, roughly one of every four CS major students does not have any idea about major security threats. For the non-science majors, these numbers are even bigger: every three students out of four are ignorant in security related problems. We consider these numbers to be very high.

Teaching cyber security is the point where out secure future starts. But just giving students more detailed information about the methods of resolving security problems cannot significantly change the situation. Well-known saying states:"If I know what I don't know, I can learn it". In our case, we can rephrase it:"If I know what I don't know and I believe it is important to know, I will learn it". We believe security education has to include security related material going side-by-side with motivation to learn these materials. It should contain more case studies and examples related to the materials explained. Without doing this, it is very difficult to motivate 75% students with non-science majors and 25% of students with CS majors to study and follow security rules. Together with implicit incorporation of security into existing courses [1,2], motivation will increase the awareness of the users and developers about security problems.

Of course, motivation is important for every educational process. What makes it so special for teaching security? There are a great number of various security threats available. Even now, it is hard to remember all of them. But, literally, every day brings more and more threats. It is not possible to teach students how to defeat all of them. We have to create in our students a permanent type of behavior according to which they will be motivated to anticipate the security threats and constantly study security. Failing to do this may form a potentially dangerous situation for a computer user. For a professional in the computer area, not following security rules is even more risky because this may affect many people at the same time.

Conclusion

In this paper we have considered the emerging problem of security education: how to motivate the students to learn security. Our research shows that many students (both having CS and non-CS majors) are unaware of security problems and threats. These students need additional motivation to study security. More examples and "security stories" should be

included in the teaching process, and we believe this will diminish the number of students who answer "I don't know" to security related questions.

References:

[1]. M Bishop, *"Teaching Security Stealthily",* IEEE Security & Privacy, vol. 9, no. 2, 2011, pp. 69-71.
[2]. K. Nance, "*Teach Them When They Aren't Looking: Introducing Security in CS1*," IEEE Security & Privacy, vol. 7, no. 5, 2009, pp. 53–55.

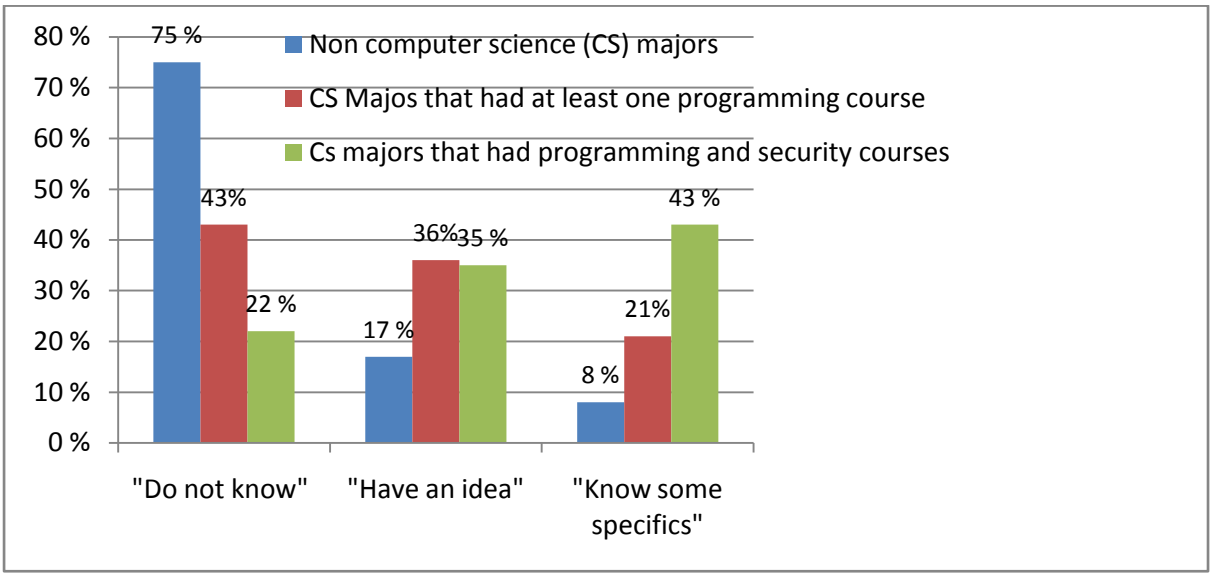

Figure 1 Percentage of the students answering network security questions in different answer categories

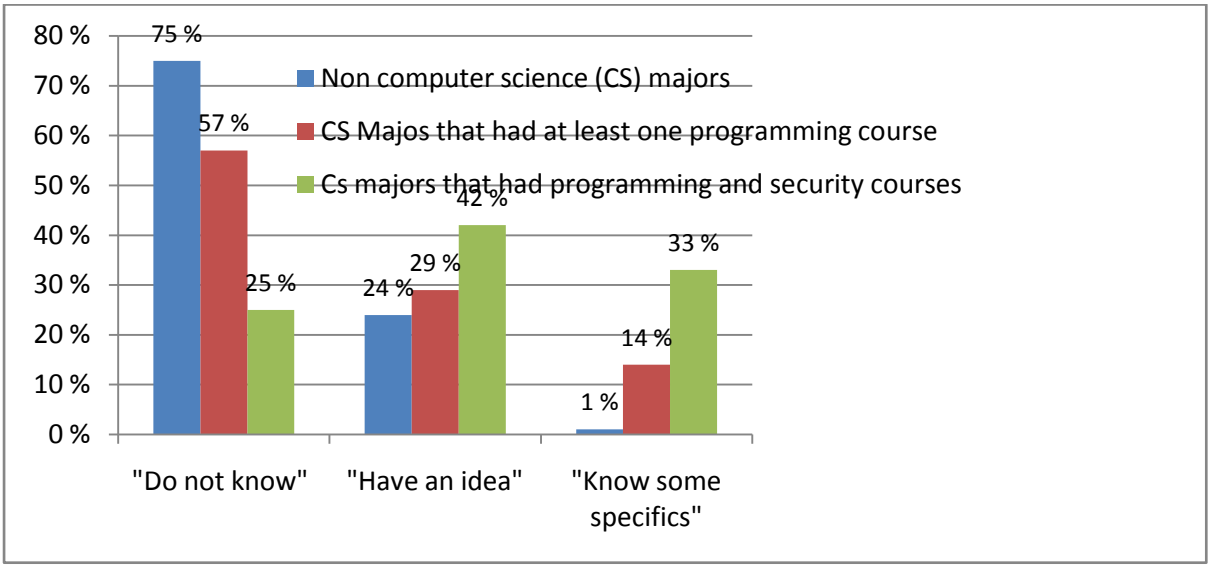

Figure 2 Percentage of the students answering software security questions in different answer categories