Training Students to Steal: A Practical Assignment in Computer Security Education

Trajce Dimkov, Wolter Pieters, Pieter Hartel
Distributed and Embedded Security Group
University of Twente, The Netherlands
{trajce.dimkov, wolter.pieters, pieter.hartel}@utwente.nl

ABSTRACT

Practical courses in information security provide students with first-hand knowledge of technical security mechanisms and their weaknesses. However, teaching students only the technical side of information security leads to a generation of students that emphasize digital solutions, but ignore the physical and the social aspects of security. In the last two years we devised a course where students were given a practical assignment which includes a combination of physical security, social engineering and digital penetration testing. As part of the course, the students stole laptops using social engineering from unaware employees throughout the university campus. The assignment provided the students with a practical overview of security and increased their awareness of the strengths and weaknesses of security mechanisms. In this paper we present the design of the practical assignment and the observations from the execution.

Categories and Subject Descriptors: K.3.2 [Computer and Information Science Education]: Computer science education;

General Terms: computer crime, computer science education.

Keywords: computer security education, laptop theft, penetration testing, physical security, social engineering.

1. INTRODUCTION

Educational institutes are starting to offer specialized CSIA (Computer Security and Information Assurance) courses, designed to train students in assessing and improving the security of digital systems. Computer security focuses on the protection of data from theft and corruption by using a combination of physical, digital and social mechanisms. Physical mechanisms focus on restricting and detecting physical access to the data, such as locks, CCTV, infrared sensors and heat sensors. Digital mechanisms focus on digital detection and protection of the data. Common digital mechanisms are firewalls, intrusion detection systems and encryption. Finally, social mechanisms focus on increasing the security awareness of the employees and reducing mistakes from human factors. Examples of social mechanisms that improve security are lectures on social engineering and clearly defined policies.

Graduate courses in computer security often provide a narrow view on security and focus mostly on the digital aspects (Figure 1, dashed line). Such a focus provides an unrealistic view of the security requirements of an organization and leads to students assuming that digital means ensure secured data. A recent study by the Threat Assessment Center [1] shows that 87% of the attacks performed by insiders required no technical knowledge and 26% of the insiders used physical means or the account of another employee as part of the attack. In the literature there are numerous examples where an adversary uses social engineering and physical access to obtain data [2, 3, 4]. Thus, it is important to get the students acquainted with attacks in which the hacker uses also physical and social means to compromise the data (Figure 1, solid line).

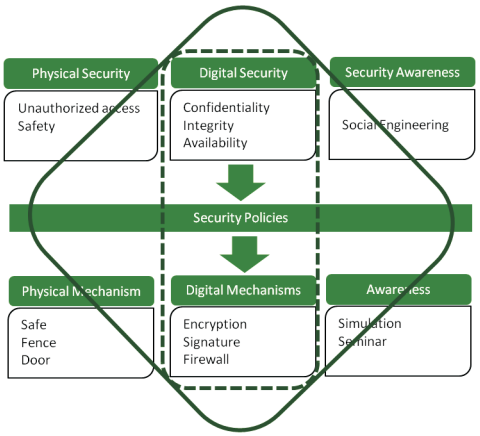

Figure 1: Computer security in context

Practical assignments clarify and support the theory students learn. In practical assignments students use the same methods and tools that hackers with malicious intent use to gain access to information. The usage of practical assignments in computer security is performed as part of many computer security courses, such as in forensics [5], in education on spam [6] and in social engineering [7]. We believe that students need to understand the hacking mentality and see how an adversary would attack also in the physical and the social domain of information security. That can be done by giving students first hand experience of the effectiveness

SIGCSE'11, March 9–12, 2011, Dallas, Texas, USA.

of the physical and social security mechanisms, exploring which attack vectors are more likely to succeed than others.

In this paper we present the practical assignment of an introductory graduate course in computer security. The goal of the course is to give a broad overview of security to the students and to increase their interest in the field. As part of the course, the students steal laptops from unaware employees, mount offline attacks on the laptop and attack a vulnerable server using the data from the laptop.

In section 2 we present the course and give a description of the practical assignment as well as observations from the execution of the assignment. In section 3 we present in greater detail the practical and ethical implications of the physical penetration test from the assignment. In section 4 we summarize our experience.

2. COURSE DESCRIPTION

Since 2008 we have taught a class on introduction to computer security to graduate students. The duration of the course is eight weeks, in which the students need to write a scientific paper and take part in a practical assignment which can be either suggested by them or by the lecturer. The course is part of a master track in computer security, and introduces the students to all concepts in security. The rest of the courses in the security track provides in-depth knowledge in different aspects of information security. The goal of the introductory course is threefold:

1. Describe important concepts in computer security from the perspective of physical, digital and social security.
2. Prepare the students to place security mechanisms in an overall security context; for example, design a system or analyze a situation and determine what the different physical, digital and social mechanisms could achieve in a given scenario or what techniques could be applied to reach a given goal.
3. Provide students with a first-hand experience with the strengths and weaknesses of security mechanisms from the physical, digital and social domain.

As part of the class, we provide a practical assignment where the students take the point of view of an adversary.

Figure 2: The steps in the practical assignment

The practical assignment is divided in three exercises, (1) physical penetration exercise using social engineering, (2) offline attacks on a laptop and (3) online attacks on a vulnerable server (Figure 2).

The goal of the physical penetration exercise (1), which follows the methodology described in [8] is to make the students aware of the social engineering and physical activities an attacker can use to get sensitive data, by stealing a laptop. After this exercise the students should have knowledge of social engineering and physical security, and know the threats that arise from them.

During the digital penetration testing exercise, the students need to get access to encrypted data residing in a laptop (2) and use the data as an attack vector in online attack on a vulnerable server (3). The goal of the exercise is to give the students an overview of the current offline and online techniques in compromising a system. After the exercise, the students should to be able to use the common tools used in penetration testing, and know their capabilities. In 2008 we performed a pilot study using practical assignment with nine students divided in three groups. After positive feedback and applying the lessons learned in the pilot study, we gave the practical assignment to all students in the class of 2009, eleven groups of three students.

2.1 Design of the practical assignment

To set up the environment for the practical assignment, we used 11 marked laptops and deployed 11 servers in which we introduced a few vulnerabilities. On each of the laptops we put two copies of a file containing the IP address of one vulnerable server. One copy was encrypted with WinZip[1] and the other with TrueCrypt[2].

We distributed the laptops to 11 unaware employees in nine buildings. The employees were recruited through snowball sampling [9]. As a cover story, we told the employees we were performing a usability study of laptops, and needed to record the results using web-cameras. Telling the employees about the real nature of the assignment would have made them overprotective of the laptops. Each employee signed an informed consent, upon which we gave them a laptop, a Kensington lock and a web-camera.

Each laptop was protected with at least three layers of access control: the entrance of the building, the entrance to the office of the employee and a Kensington lock.

After setting up the environment, we gave each of the teams the location of a single laptop they should obtain. First, each team scouted their location and collected as much information as possible about the employee and the security mechanisms in place. Then, each team proposed a list of attack scenarios they wanted to conduct. Each scenarios was approved by us and the security management. The students had two weeks to gain possession of the laptop.

The actions of the teams were logged using the web-cameras we positioned in the offices of the employees and through recording devices carried by the students, such as mobile phones. We used such comprehensive recordings to be sure the employees were treated with respect by the penetration testers. After each successful or failed attempt, the teams provided an attack trace listing which mechanisms they circumvented and, in case of failed attempts, which mechanism caused the attack to fail.

In the second exercise from the assignment, the students used offline attacks, such as the coldboot attack [10] and/or password cracking tools such as John the Ripper[3] and Hydra[4] to obtain the IP address from the encrypted file. In the last exercise the students used Backtrack[5] to attack the vulnerable server and obtain a protected file.

In this paper we focus only on the first exercise of the assignment, the physical penetration test. The second and

[1]www.winzip.com
[2]www.truecrypt.org
[3]www.openwall.com/john
[4]freeworld.thc.org/thc-hydra
[5]www.backtrack-linux.org

third exercise can be considered as a reproduction of exercises reported by other authors [5, 11, 12].

2.2 Results from the physical penetration tests

In both academic years, all groups managed to gain possession of the laptop. Besides the 3 successful attempts in 2008 and the 11 successful attempts in 2009, there were 11 unsuccessful attempts. During the tests, students took on roles as course assistant, help desk worker, PhD or graduate student or even a film crew in their social engineering attacks. The main targets of the social engineering were the employees who possessed the laptop and the support staff such as the secretaries, janitors and people from the cleaning service.

Figure 3: The student (left) went to the janitor (right) with a spoofed email stating that they need to pick up a laptop. The janitor unlocked the office with the laptop and helped the students find the key of the Kensington lock.

In nine cases the employees gave the laptop either after being showing a spoofed email or being promised they would get the laptop back in a few hours. However, in five cases the students were not able to social engineer the employee directly and were forced to look for alternative approaches, such as social engineering the janitor (Figure 3) or an employee from the cleaning service (Figure 4). The complete results from the penetration tests are presented in [13].

2.3 Observations

Running the practical assignment is challenging. We had difficulties in attracting employees to participate in a study where they are not told what the exact goal is. Recruiting employees becomes even harder the following years, when more people know about the exercise, and therefore are not eligible as participants. This makes the exercise more suitable for larger universities, which have more employees.

Another problem we encountered is positioning the web-cameras. A web-camera requires all employees in the office to agree with its presence, a desktop to store the data, and administrative rights on the desktop. Only a few employees had a desktop, and even fewer had administrative rights.

Another concern we had was debriefing the employees after the exercise. During the debriefing we explained the benefits of the exercise and the reason why we could not inform them in advance. At the end of the debriefing all employees were given small presents. Although the employees were pleased with the exercise, we expect that this will not always be the case.

Figure 4: A student cutting a lock with a bolt cutter. The student came to the building at 7am and claimed to the employee from the cleaning service he forgot the key of his office. After the employee from the cleaning service gave the student a spare key, the student went inside the office, cut the Kensington lock with a bolt cutter and obtained the laptop.

During the assignment, we obtained a realistic picture of the physical security of the university and the security awareness of the employees. The security management discovered weaknesses in their CCTV monitoring and in the adherence to policies by security personnel.

3. IMPLICATIONS

During the design of the course, we had four major concerns. First, the execution of the assignment might violate the law. Second, the assignment is executed in an environment where the outcome cannot be controlled. Thirdly, the assignment teaches students to steal and lie. Finally, the assignment includes deceiving employees. In the rest of this section we explore the implications.

3.1 Legal implications

To ensure that we were operating within the law, before deploying the assignment we consulted the legal department of the university. Following the advice from the legal department, we forbade all scenarios that included (1) theft of any object besides the laptop, (2) searching through the belonging of the employees and (3) impersonation of officials of the university, police, fire department, etc.

3.2 Reducing unexpected outcomes

The assignment was executed on the campus of the university. This is a semi-controlled environment, where we could neither fully control the behavior of the students nor the behavior of the employees and the security personnel. We applied the following principles to the design of the exercise:

1. *Limit the scope of the activity.* The students were not allowed to use intimidation, violence nor to put the employees or themselves at risk. They were also forbidden to cause any physical damage, except for cutting the Kensington locks. The laptops were clearly marked and the students were allowed to gain possession only of a specific laptop. All students signed the rules of engagement before the scouting phase.
2. *Control the risk.* All attack scenarios were approved in advance by us, and only minor deviations in the ex-

ecution were allowed. The web-cameras and the students recorded with video/audio of all their activities. The recordings allowed us to see if the employees were treated with respect or were put at risk. Finally, all students were given a lecture on the ethical aspects of social engineering and theft.

3. *Reduce the impact of the exercise.* Just after the execution of the task, the students reported to us. When the laptops were stolen without knowledge of the employees, we tried to inform the employees before they found the laptop gone. The employees were briefed from the beginning not to store any sensitive, private nor critical information on the laptops, and to use them only for gaming and surfing. At the end of the assignment, we properly debriefed all the employees, and provided small gifts for the participation.
4. *Introduce escape clauses.* The employees and the students participated voluntarily in the study. Both groups were aware, and signed an informed consent stating they can stop with the activity at any time. All students were given "get out of jail" cards in case they are caught by the security guards. The cards contained phone numbers of the security management and the lecturers. The security management had information about all the target employees and all the students who participated in the exercise.

3.3 Ethical implications for the students

During the design of the first part of the assignment, the physical penetration tests, we were concerned (1) whether the students would feel comfortable with the activity and (2) whether we were training a future generation of criminals.

Benefits:
1. Practical in-depth overview of all aspects of security.
2. Awareness of the strengths and weaknesses of security mechanisms.
Risks:
1. Reduced comfort level of the students.
2. Misuse of the knowledge.

Figure 5: Risks and benefits from the assignment to the students

3.3.1 Comfort level of the students

Before the start of the assignments, all the students were given the opportunity to perform an experiment of their choice instead of participating in the assignment. The only limitation was that the experiment should have the same workload as the assignment. All the students decided to join the assignment.

Survey among the students

To evaluate their level of comfort we devised two questionnaires, one before the exercise and one after the exercise. We had 31 respondents (94%) for each of the questionnaires. The students graded on a scale of 1 (strongly disagree) to 5 (strongly agree) how much they agree with a statement.

The majority of students felt comfortable during the assignment. The number increased from 65% before the execution of the exercise, to 77% after the exercise. Most students thought the assignment would be fun, but the percentage dropped from 71% to 65% after conducting it. At the beginning students felt less comfortable because they were not sure what kind of attacks they would perform. After we approved only the low risk scenarios, the comfort level increased, but the fun part of the activity decreased. 68% said they would repeat the assignment if they were again given the chance. The results are summarized in Figure 6.

Question	Av.	SD
Before the exercise:		
The exercise will be fun	4.6	0.7
The exercise is useful	4.1	0.8
I feel fine about the exercise in general	3.8	1.1
I feel fine about the ethical implications of the exercise	3.5	1.2
After the exercise		
The exercise was fun	4.5	0.7
The exercise was useful	4.1	0.9
I feel fine about the exercise in general	4.1	1.0
I feel fine about the ethical implications of the exercise	3.6	1.2
I would do the exercise again	3.9	1.2
I am now more aware of physical and social security	3.9	0.9

Figure 6: Results from the students before and after the first part of the assignment

Year:	2008	2009
Respondents:	40 (100%)	28 (90%)
1. The course was well organized	7.4	8.6
2. My attendance was above 80%	7.3	8.9
3. I liked the practical assignment	5.6	8.2
4. Overall grade of the course	6.8	7.8

Figure 7: Results from the students after passing the course

The students filled out another questionnaire after finishing the course, as part of the standard quantitative evaluation of courses in the university. The results show the satisfaction of the students increased as well as their attendance in class compared to the previous year (Figure 7). The grade of the course increased a whole point, from 6.8 in 2008 to 7.8 in 2009, thanks to the enthusiasm of the students for the practical assignment. The average grade of the rest of the courses were 7.2, both in 2008 and 2009.

3.3.2 Risks of teaching students to steal

Checking if we are teaching the next generation of criminals is a more subtle issue. The benefit of educating students in the adversarial aspect of security is widely discussed and implemented in many security courses. Pashel [14] and Logan and Clarkson [15] discuss the ethical implications of teaching students to hack and the possibility of misusing the acquired knowledge. We show that the arguments in favor of teaching digital penetration testing also hold for the physical domain, by establishing an analogy between digital and physical penetration testing.

Analogy to teaching digital penetration testing

According to Pashel [14] and Logan and Clarkson [15], teaching hacking to students is mostly justified, because to provide the best security defense, a system administrator

Question	Average	SD
1: Deceiving the subject	3.5	1.2
2.1: Physical damage - Discomfort	2.3	1.1
2.2: Physical damage - Injury	1.3	0.8
2.3: Physical damage - Death	1.0	0.0
3.1: Material damage - Emotional	2.4	1.2
3.2: Material damage - Financial	2.8	1.3
3.3: Material damage - Production loss	2.1	1.4
4.1: Psychological damage - Threats	2.1	1.0
4.2: Psychological damage - Deception	4.2	0.8
5.1: Privacy - Assume identity	4.0	1.0
5.2: Privacy - Access sensitive informa.	3.6	1.3
5.3: Privacy - Destroy information	2.3	1.1
5.4: Privacy - Theft of information	3.2	1.3

Figure 8: Ethical acceptability of damage according to students

must possess the same skills as the attacker. We consider this to be the *Locksmith Argument*. For any locksmith to be able to create decent locks they also need to have the ability to break locks (or at least have extensive knowledge on the techniques of a lock picker). The same argument can be applied to teaching physical penetration testing. The only way a student is able to secure physical objects is to have extensive knowledge on how attackers penetrate organizations, buildings and so forth. Letting them gain experience from an attacker's point of view will positively affect this knowledge.

Another argument in favor of teaching students digital penetration testing is that these skills are useful in discovering weaknesses in the security of a system [15]. The same argument can be applied to physical penetration testing. For example, an insurance company needs to review the physical security (such as cameras and security guards) and digital security (the network infrastructure that controls the cameras, the locks and the alarms) of a museum before determining the insurance premium.

Survey among the students

In the questionnaires we gave to the students, we also asked for their opinion on ethical issues. The students were told to assume there were no rules in the assignment, the only objective was to obtain the laptop.

We asked what type of damage the students are willing to inflict on the employee or the surroundings: physical, material, psychological damage and invasion of privacy. Each type of damage consists of some subtypes that contain examples of such damage, varying from light to severe (in our perception). In this way, we could identify the ethical sensitivity of types of damage, in the perception of the students.

The results from this survey are shown in Figure 8. The scale is from 1 (uncomfortable / I will never do that) to 5 (comfortable / I have no problem doing that). The questionere was filled out by 28 students(85%).

Physical damage is a sensitive matter. Even light physical damage or emotional damage was rated only around 2. The roots for this rating can be found in the basic ethics of society e.g. "do not hurt people" and "respect your fellow human beings". The students are less concerned with material damage than physical damage. Ratings are rather spread with this type of damage: some students do not care about material damage at all while other students do feel very uncomfortable causing material damage. It is surprising to see that the students feel uncomfortable with causing production loss.

Furthermore, threats and intimidation are again sensitive according to the students: The rating averages around 2. Deception however does not seem to be such a big problem, most students have no difficulty in feeling comfortable with deceiving the employee. It is also surprising to see that privacy issues do not make the students feel very uncomfortable. Destroying information does rate as very uncomfortable, but other types of privacy issues tend to rate toward comfortable.

3.4 Ethical implications for the employees

Baumrind [16] considers deception of subjects in testing as unethical. The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, also clearly states this in their first rule of ethical principles: "Respect for persons" [17].

Benefits:
1. Increased awareness of the employees.
2. Checks the security mechanisms in the university.
Risks:
1. Employees are deceived.
2. Employees or their data might be put at risk.

Figure 9: Risks and benefits from the assignment to the employees

However, in some studies deception of the participants cannot be avoided. Finn [18] defines four conditions that need to be met to make deception acceptable: (1) The assessment cannot be performed without the use of deception. (2) The knowledge obtained from the assessment has important value. (3) The test involves no more than minimal risk and does not violate the rights and the welfare of the individual. Minimal risk is defined as: "the probability and magnitude of physical or psychological harm that is normally encountered in the daily lives" [19]. (4) Where appropriate, the subjects are provided with relevant information about the assessment after participating in the test.

Physical penetration testing using social engineering can never be completely respectful because it is based on deception. However, the deception used in the assignment presented in this paper is justifiable.

The first two conditions are general for penetration testing and its benefits, and have been discussed earlier in the literature (for example, Barrett [2]). The third condition states that the risk induced by the test should be no greater than the risks we face in daily lives. Students cannot physically harm the employee because of the rules of engagement, thus only psychological harm is possible. If the employees help the student voluntarily, the risk of psychological harm is minimal. The logging equipment assures the interaction can be audited in case of dispute. The only case when the risk is above minimal for the employee is if the student gains possession of the asset without knowledge of the employee. When the employee finds the asset missing, her stress level might increase. Therefore it is crucial for the lecturers to debrief the employee before the employee learns about the theft. The fourth condition states that all employees should be debriefed after the assignment. All employees signed an informed consent and are debriefed after the assignment.

Survey among the employees

Nine employees (82%) from which the students obtained the laptop filled a questionnaire after the debriefing. They answered multiple questions, on a scale of 1 (I strongly disagree) to 5 (I strongly agree) and yes/no questions. The results are summarized in Figure 10.

About 60% of the employees said that the university should continue letting graduate students perform these assignments and most of them, 89%, also agreed that these kinds of assignments can improve the security awareness, both that of the students and of the university employees.

Question	Av.	SD
1. I found the exercise interesting	3.2	0.9
2. The exercise increased my awareness	2.5	1.4
3. The exercise should be done more often	3.0	1.0
4. During the exercise I found myself stressed	1.0	0.8
5. I find the assignment ethical	3.0	1.1
6. These exercises are harmful	1.0	0.4
7. These exercises will benefit students	1.8	0.5
8. The security awareness of students and employees can be improved through such exercises?	4.5	1.5

Figure 10: The view of the employees

4. CONCLUSION

To make students aware of physical and social aspects of security, these aspects need to be included in security courses, both from a theoretical and a practical point of view. We presented a practical assignment consisting of three steps. First, the students needed to steal a laptop from an unaware employee, then decrypt a document from the laptop, and finally use the information from the document to attack vulnerable servers.

The students enjoyed the assignment and their awareness of the physical and social aspects of security increased. During the course they learned the strengths and weaknesses of common physical, digital and social mechanisms used to secure sensitive information. Such experience is essential for the future security architects and chief security officers. Furthermore, the practical assignment increased the overall attendance in the course and improved the course grade.

However, the assignment is challenging to administer and draws ethical and legal implications. The students might feel uncomfortable to execute the attacks or the employees might not be treated with respect. The students might also abuse the new skills in illegal actions.

Surveys among students and employees indicate that the risks can be managed. Employees who participated in the exercise did not feel stressed nor considered the exercise harmful. Moreover, the arguments used in favor of digital penetration testing also apply for physical penetration testing. Therefore, we believe the benefits of the practical assignment outweigh the mentioned risks. This assignment can be used by other universities in introducing computer security to graduate students.

References

[1] M.R. Randazzo, M. Keeney, E. Kowalski, D. Cappelli, and A. Moore. Insider threat study: Illicit cyber activity in the banking and finance sector. *U.S. Secret Service and CERT Coordination Center Software Engineering Institute*, pages 1–25, 2004.

[2] N. Barrett. Penetration testing and social engineering hacking the weakest link. *Information Security Technical Report*, 8(4):56–64, 2003.

[3] K.D. Mitnick and W.L. Simon. *The Art of Deception: Controlling the Human Element of Security*. Wiley, 2002.

[4] W. Allsopp. *Unauthorised Access: Physical Penetration Testing For IT Security Teams*. Wiley, 2009.

[5] L.L. DeLooze. Counter hack: Creating a context for a cyber forensics course. In *FIE'08: Frontiers in Education Conference*, pages 1–6, New York, 2008. IEEE.

[6] J. Sommers. Educating the next generation of spammers. In *SIGCSE'10: Special Interest Group on Computer Science Education*, pages 117–121, Wisconsin, USA, 2010. ACM.

[7] B. Endicott-Popovski and D.L. Lockwood. A Social Engineering Project in a Computer Security Course. *Academy of Information and Management Sciences Journal*, 9(1):37–44, 2006.

[8] T. Dimkov, A. Cleef van, W. Pieters, and P. Hartel. Two methodologies for physical penetration testing using social engineering. In *ACSAC'10*, Chicago, USA, 2010. ACM.

[9] B.L.A. Goodman. Snowball sampling. *The Annals of Mathematical Statistics*, 32(1):148–170, 1961.

[10] J.A. Halderman, S.D. Schoen, N. Heninger, W. Clarkson, W. Paul, J.A. Calandrino, A.J. Feldman, J. Appelbaum, and E.W. Felten. Lest we remember: Cold boot attacks on encryption keys. *USENIX Security*, pages 45–60, 2008.

[11] A.M. Minkley. Cyberattacks: a lab-based introduction to computer security. In *SIGITE '06: Proceedings of the 7th conference on Information technology education*, pages 39–46. ACM, 2006.

[12] J. R. Aman, J. E. Conway, and C. Harr. A capstone exercise for a cybersecurity course. *Journal in Computing in Small Colleges*, 25(5):207–212, 2010.

[13] T. Dimkov, W. Pieters, and P. Hartel. Effectiveness of physical, social and digital mechanisms against laptop theft in open organizations. In *IEEE/ACM International Conference on Cyber, Physical and Social Computing*. IEEE, 2010.

[14] B.A. Pashel. Teaching students to hack: ethical implications in teaching students to hack at the university level. In *InfoSecCD '06: Proceedings of the 3rd annual conference on Information security curriculum development*, pages 197–200, NY, USA, 2006. ACM.

[15] P.Y. Logan and A. Clarkson. Teaching students to hack: curriculum issues in information security. In *SIGCSE'05: Special Interest Group on Computer Science Education*, pages 157–161, Missouri, USA, 2005. ACM.

[16] D. Baumrind. Research using intentional deception. Ethical issues revisited. *The American psychologist*, 40(2):165–174, 1985.

[17] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. The Belmont report: Ethical principles and guidelines for the protection of human subjects of research. pages 1–18, 1978.

[18] P.R. Finn. *Research Ethics: Cases and Materials*, chapter The ethics of deception in research, pages 87–118. Indiana University Press, 1995.

[19] Code of Federal Regulations. Title 45: Public welfare department of health and human services. part 46: Protection of human subjects. pages 1–12. 2005.