E-learning of ethics, awareness, hacking and research
by information security majors

J. A. Koskinen
Lecturer
Tampere university of technology
Tampere, Finland
E-mail: jukka.a.koskinen@tut.fi

Keywords: information security, ethics, hacking, research

INTRODUCTION

Some earlier courses were reorganized in 2013 to construct a curriculum for the information security major at Tampere University of Technology (TUT). This paper describes how the compulsory courses introduce four important non-technical engineering skills using mainly an e-learning approach. This approach (i) saves resources in the beginning – while large number of students head for other majors – and after that (ii) offers flexibility in scheduling to serve the elective courses, as well as the studies of other disciplines – those that provide a need for security. The four skill areas are (E) ethics of individuals and organizations, (A) people's awareness of security issues, (H) hacking, i.e. offensive way of thinking, and (R) research, i.e. productive scientific approach. One of the main points of this paper is the repeated exposure of students' minds to various ways of thinking. The described introductory stage of exposing them to the EAHR matters does not forget innovativeness, but that remains more in the background before the students start working with cases and hands-on experiments later. Besides EAHR we will make heavy use of another acronym: Information Security is shortened as IS. After discussing some background, we describe the four courses, first as part of the whole IS curriculum, then as users of e-learning and then separately from each of the EAHR points of view.

1 NON-TECHNICAL SKILLS IN INFORMATION SECURITY

1.1 General remarks

This paper concentrates on such non-technical skills that deserve special attention in the field of IS. At TUT and elsewhere the engineering students will learn languages, oral and written communication, group interaction, leadership etc. Such soft skills in information technology are discussed in [1] based on ACM and IEEE recommendations, psychosocial research and student surveys. Our curriculum developed gradually from two IS courses in 1999, reached the size of a minor subject in 2003 and became a major subject in 2013 after many additions and frequent adaptations to what seemed to be useful for the purpose of successful IS professionals. Pedagogical principles were followed, comparisons were made to IS curricula elsewhere, and re-

search on technical IS affected the curriculum. The "soft side" of the curriculum, however, developed without much reference to educational reports like [1]. *Emotional intelligence* is named in [1] as an underlying factor for the soft or non-technical skills in engineering and also in information technology: it is "a measure of the ability to assess and control both oneself and others." Of course the IS curriculum shares responsibility to promote such skills, but they are more readily found in the learning outcomes of the whole engineering degree. While we now focus on the special cases of EAHR, we note that E, A and R can also be considered skill areas not specific to IS. One of our main points is that these areas deserve special attention in IS, and hacking, which is in a way endemic to IS, also belongs to the soft side.

We would like to motivate the discussion of EAHR by noting that these skills have a *first* and a *second order*. First, be ethical and aware yourself so that you can take care of your IS. After that you can develop understanding how ethics and awareness work in others, whence you can design systems – including policies and legislature – that make it easier for others to act correctly and more difficult to do otherwise. For hacking this is even more apparent: being yourself able to hack helps you to anticipate how hackers might work against your designs. Finally, to understand research is not only about being able to carry out research yourself but to be able to interpret research results to improve your designs. It is the 2nd order that motivates EAHR for IS.

1.2 Ethics

In [2] there are five suggested high-level outcomes of cyber security in an information technology curriculum. The fifth one is: "Students will understand the ethical responsibilities of the cyber-security profession and will treat ethical, moral and privacy issues responsibly and with sensitivity." Dark et. al [3] have created a framework for IS ethics education, and they propose a very thorough treatment of ethical issues within this framework – partly motivating even the study of technical measures from this point of view. Their proposed learning activities exceed the practices and possibilities of our courses. Still it will be useful to let the students become aware of the meaning of their ethics-related course activities within this framework.

1.3 Awareness

Awareness of IS seems not to be a big concern for those who are on IS courses. This is true only for their own awareness and only in the short perspective. The field of IS is actually a battlefield where there often happen major unpleasant breakthroughs, constantly smaller breaches, and sometimes important development in protections. This is why the student should develop a habit of being constantly aware of changes in the field. This is not possible if not accompanied by an ability to filter out irrelevancies. And, the more you are aware of the current events the easier it is to know what is relevant. The skills of managing large quantities of well-organized information and constantly being able to adapt to new situations goes beyond the topic of the current paper, but evidently they are essential non-technical skills also for IS engineers. Furthermore, a specific branch of adaptability belongs to the area of the emotional intelligence and is very important for IS. It is endurance of pressure: IS professionals that work in the front line of defence in organizations must not panic.

What was said above concerned the first-order awareness, i.e. knowing about one's own IS and its risks and knowing how to deal with them – and hopefully also having a suitable attitude to take proper actions. It is a growing field of research to investigate the IS awareness and the ways to improve it, especially in organizations but more and more also in the ubiquitously computing society. The increase in awareness research is motivated by the fact that technical IS solutions are less and less sufficient as the number and variety of users increase. This has led even to

suggestions of complementing technical IS with *societal IS culture* [4]. It has been also noted in [5] that “there has been a trend of making IS “softer” by focusing on cultural aspects” and the trend also shows “in an increased emphasis on awareness campaigns in several companies”. Interviews related to such campaigns form the source of the analysis in [5]. In our current context treatment of IS culture, whether organizational or societal, means the second order. It is mainly about “A”, but touches also “E” and “R”. It is obviously useful to let the students gain an understanding of the second order issues while they are developing their own awareness.

1.4 Hacking

One of essential skills of a defender is the ability to think like the offender. In [6] it is put forward even that “teaching ethical hacking techniques is becoming a necessary component of computer security curriculum as it yields better security professionals than other curriculums teaching defensive techniques alone.” Especially this means that hacking must be more offensive than the ideal creative exploration of technology that helps pushing it in new directions. The mind-set the student should temporarily attain is that the directions are just inwards with no motivation to advance science or technology. A branch of IS professionals, the penetration testers, get their living directly from such behaviour. So do many criminals, and this is why ethics is an essential ingredient that must go with any sort of hacking activities. Comparing to recommendations of [6]: We do have (i) discussions of legal implications and ethics, and an understanding why the techniques are studied, and (ii) the laboratories used are isolated from all networks outside the classroom, as well as from the Internet, but (iii) our students do not sign a code of conduct during the course registration and (iv) the students are not screened for criminal background, unstable behaviour or malicious activities prior to admission to the IS courses. Our students are only restricted by the university-wide boundaries for student behaviour and the consequences for unacceptable behaviour.

1.5 Research

It is well known that security engineering has the unique characteristic among engineering fields: It does not suffice to make the designs safe or even fool-proof. They must be proofed also against active adversaries. These adversaries find and exploit vulnerabilities, and in doing so they are conducting research. In this sense research should be included already through the hacking point of view – even though a hacker’s research can be very narrow-minded, because the first working solution suffices. Seen from the other side, in order to be able to defend, new methods must be found and this means that the defender must understand how research is done. This is part of the often-mentioned ongoing battle between good and bad and it applies to competition among all sorts of rivals. The IS studies cannot ignore it either.

2 THE CONTEXT FOR EAHR IN FOUR COURSES IN THE CURRICULUM

2.1 IS curriculum

The major subject of IS at TUT is a 30 ECTS credit unit (cu) package in the master’s degree. That degree consists of 180 cu’s, plus an underlying bachelor’s degree of 120 credit units. As their other subjects the students may have for instance communications or software engineering, or information management. Some security matters are introduced to all students right in the beginning of their studies. Also the first course dealing with IS belongs to the first half of the first year. That course bears the name "Computer networks and data security" and out of its 4 cu scope about 1 cu is devoted to IS. This course is not included in the 30 cu’s of the major subject, but it is an important prerequisite. Some students continue with the first courses of the

major subject well before their bachelor's degree is ready. This is allowed and also motivated because those courses can also be included in some other subjects and they can provide the students help in choosing their major.

We shall hereafter use the number #1 for the above course. Similarly we number the three compulsory courses of the major subject:

#2. Information Security (2 cu)
#3. Daily IS (4 cu)
#4. Computer and network security (8 cu)

As the course size grows exponentially from #1 to #4, the number of students goes inversely: approximately 400, 100, 50 and 25 per year. The courses #1–#4 form a prerequisite chain. It takes at least two years to complete all courses; 3–4 years is more normal. The elective courses for the IS major are:

Security in Networks (5 cu)
Secure Programming (3 cu)
Identity and Access Management (4 cu)
IS Management (4 cu)
Mathematical Cryptology (7 cu)
Dependable Industrial Control Systems (5 cu)
Risk Management (4 cu)

Five of these are quite specialized on certain areas in IS, but they still require only #2 as their prerequisite. This is to allow them to be elected in some other subjects (like software, networks, maths). This is one reason why the small course #2 exists. Two courses in the electives list do not mainly deal with IS, but they let the student complete the major with orientation towards management or automation.

2.2 Organization of courses #1, #2 and #4

The text materials for #1, #2 and #4 are in a database that can be publicly accessed with a web application. For each page the database has a collection of multiple choice questions (1-out-of-4). Approximately 40% of them are publicly visible and the rest are hidden. The exams are made from these problems by using approximately half public and half hidden questions. The hidden questions are mostly variations of the public ones, but there are also completely different ones. Course #1 also has essay questions in the exam but only for its network content. Course #4 uses the multiple choice questions only for its midterm exam, which is optional for the students; a good score gives, however, substantial advantage for the final exam.

Similarly as with the midterm exam in #4, the students of #1 and #2 can collect advance points for the final exam. There is a web application containing about 30 small exercises with automatic assessment. Most of the exercises for #2 are multiple choice questions based on some reading tasks, whereas #1 has more practical exercises. A simple example is the removal of a single cookie from the browser. The automatic exercises provide an optional exposure to "A" and "H" on course #1. Exposure to "E" on #1 is required through the exam where questions on laws appear, and the situation of "E" and "A" is similar on #2. See more in section 3.

Course #1 is a mass course for all freshmen of information technology. The IS topics are partly interleaved with the network matters but mostly separately lectured. Course #2 lets the students learn all general concepts and methods of IS. They can do this at the time most suitable for them, as long as it is prior to #3. Most of the contents of #1 and #2 is about facts, but some more space is left for critical thinking in #2. This is however done only by contemplative texts inside the course material. The assessment of #2 happens completely with the multiple choice questions, and they do not lend themselves for evaluating very high level mental processes. Still, the questions are not merely about remembering facts.

2.3 Organization of course #3

While #2 requires isolated self-studying, #3 flows in constant interaction of groups of 6–8 students, meeting only virtually, though. As #3 is a substantial platform for the EAHR, Table 1 summarizes the main part of it. Letters E, A, H, R point out where these issues appear most. More details are given in section 3, where also the main venues for "A" and “H” in #3 are described. The materials for #3 consist of assignments and fairly brief background texts. Students access these and write their reports through the Moodle platform. Course #3 appears in its earlier form in [7]. The current version was updated to be two times larger and more professionally oriented.

Table 1. Tasks bound to a weekly schedule of course #3

Week		**Discussions** = contemplate, find and deal with info			**Exercises** = deal with people, gadgets, systems
1		Your background and objectives			Evaluate credibility of web pages (pick real and fake ones from list)
		Web archives and caches			PGP 1: install the program, create a key pair
2	(A)	Your own information security			PGP 2: obtain signatures for your key
	E	You own ethical questions			Invent+evaluate ways to create passwords
	R	Familiarization with the research task			
3		Consequences of information crimes			PGP 3: use your key to send and receive
	E,H	Ethical hacking		R	Research interviews (at least two out of five)
	R,(H)	Invent ideas beyond current research			
4		Immaterial rights (incl.your own)		A	Security practices of someone who serves customers (choose from list of service types)
	(E)	DRM protections + their weaknesses			Configure a firewall (your own + alternatives)
	E	Dubious web content		R	Remaining research interviews
5	E	Freedom of speech		H	Passwords from captured traffic (+ more)
		Experiences of web transactions		H	Security issues of self-made active web pages (sample PHP pages given + alternatives)
		Email spam			
6		Businesses | Occupations in IS			Securing WLAN (your own + alternatives)
	R	Analyse compiled research material		A	Evaluate recent security patches
7		A public service & a social media platform			Security procedures for customer at an internet bank (choose different than others)
	E	Information security in society			Security properties of a smartphone (choose a different phone than others)
	R	Analysis (II) of the research material			

2.4 Distribution of e-learning and EAHR

Table 2 shows with 0–3 stars how intensively e-learning is used and how learning about EAHR is approximately distributed among the four courses. Stars in parentheses indicate that the student can omit that part. The second and third column show how much work an average student is expected to use on the course and how big percentage of that is available as classroom teaching. Note that for course #1 only the IS-related hours are shown. The e-learning platforms “automatic exercises”, “exam”, “midexam” and “Moodle” were mentioned in Sections 2.2 and 2.3. The rest appear in section 3.

Table 2. Distribution of e-learning and the EAHR

Course	Nominal hours	Class hours	E-learn	E-learning platforms	E	A	H	R
#1	25	35 %	(**)	Automatic exercises	*	(*)	(*)	
#2	50	0	**(*)	Autom. exercises, Exam	*	*		
#3	100	2 %	***	Moodle, Tviit	***	**(*)	**	***
#4	200	35 %	(*)	MidExam, Wiki	*	**	***	**(*)

3 EAHR DETAILS

3.1 Ethics

For #1 and #2 ethics is mainly about legislation. For #1 this means copyright, privacy, and criminal law, and the focus is on the student's own actions or about being a victim. For #2 also laws governing IS in organizations appear in the exam, and IS and privacy policies in an automatic exercise. Five or six of the weekly discussions on #3 deal with ethics: These can be characterized as follows (referring to the rows at weeks in Table 1): issues in one's own environment (w2-r2), technology-related issues for citizens (w4-r2) and professionals (w3-r2), issues for organizations (w4-r2, w4-r3), and society (w5-r5, w7-r2). Although w4-r2 was mentioned twice, the topic itself is not so much about ethics, but students always start looking for right and wrong in this discussion. Not mentioned in Table 1, but also the topic w3-r2 touches ethics by asking, what kinds of computer crimes have occurred recently and what happened to the offended and offenders. Ethics is likely to be touched by discussions on similar or other current topics that occur during lectures of #4. Otherwise for #4, see the end of section 3.4.

3.2 Awareness

Most of the IS part of #1 could be seen as awareness training for the new students, but in the sense of the current discussion, "A" is on the voluntary side: one of the automatic exercises is a web-questionnaire similar to that in #3 (see section 3.4). After responding the students can see distributions of countable answers and a selection of text answers. For #2 awareness is mainly about getting familiar with policies, guidelines and web-sites of security information. As noted above, policies also have an ethical dimension.

Already the very first assignment on #3 tries to lead the students towards the second-order "A": They are required to find an application for IS awareness or measurement, or an IS quiz for their smartphone or computer and write a report on it. This is not in Table 1, because it is a threshold task to be completed by the 4th course day. The main "A"-promoting assignment in #3 continues through the whole duration of the course. Averagely every other day the students must write a tweet about (i) fresh news about IS with a reference and (ii) their own act or observation that concerns IS (and is not from the course only), altogether 24+24. The tweets are actually "tviits" on our own platform, but their harvest is publicly viewable at http://sec.cs.tut.fi/arki/. In Table 1 two exercises have been marked with "A" (weeks 4 and 6), because they are supposed to make the student think how others see IS: a person serving customers, and people who should be able to decide whether they need a security patch or not. Similar second-order awareness could be attributed to some other exercises, too: One example is the internet banking, but students usually confine their report to techniques and do not evaluate the human aspect. Another example is the separate assignment where the student must evaluate a text page from #2, improve a multiple choice question or create a new one, and evaluate someone else's output.

Awareness in #4 means knowing about campaigns in organizations or nations and supposedly makes students more capable of using or designing such. This already gets a little beyond non-technical skills, because IS engineers might do this at work.

3.3 Hacking

Course #1 offers one automatically checked hacking exercise: The student has to by-pass authentication by changing the source code of a web page. Course #3 requires the student to carry out a hacking exercise at his or her best level at one of listed www sites and write a report by the end of the course. In spring 2015 the students worked on these sites: www.hackthissite.org, www.try2hack.nl, www.hellboundhackers.org, www.net-force.nl, www.enigmagroup.org, hack.me.

Two of the weekly exercises in #3 provide limited kind of hacking experience: using Wireshark to find a password in captured packets and to find vulnerabilities in PHP code. The latter one is difficult for many and it has easier alternatives, like evaluating risks in deploying codes on one's own web pages. Everyone however sees in their group how the SQL injection appears in the code. The teacher is rarely needed to show this. It is also possible to accomplish the packet task and the hacking site task at very different levels of expertise. For instance the ARP spoofing that happens in the packet stream is usually found only by a couple of students if any. The password that consequently was transmitted without encryption can be found by everyone at least after reading how other members of the group spotted it in their own capture file. Regardless of the rather simple hacking achievements the students usually report elevated interest and refer to future continuation with hacking.

Course #4 has a physical isolated hacking laboratory. Besides three cryptographic exercises the students must choose two out of three hacking assignments. The two first alternatives, CSRF and XSS, are the same as in [8] and the third one “TCP/IP” is a modification from [8]. Guidance is available, but self-work is also possible. Furthermore, there is a penetration exercise against a Linux server. It uses the nmap network scanner and Metasploit Framework as the basic tools for the attack, and the students are instructed to learn in advance about the recent vulnerabilities in the openssl library (Heartbleed) and in the bash command line interpreter (ShellShock).

3.4 Research

The students of #3 have to interview five citizens about their IS practices. Students usually find suitable interviewees among their relatives or acquaintances. The biggest problem seems to fill all age categories – the ages must start with a different number. The interview means filling in a form together with the respondent that has already filled in more than half of it. The advance questions have developed towards multiple choice type, whereas the interview questions are mostly open. Some students do not meet their interviewees face to face but use a phone. There are two weeks to complete the interviews. During one week’s break the teacher collects the data into a spreadsheet, and the students work on it for two weeks. Each group is given roughly an equal share of the questions, 2–4 questions per student, choosable within the group. The first task with an open question is to categorize its answers into classes given by the teacher. In the first versions of this task the student also had to invent the classes but this was abandoned as too demanding. There have been fewer and fewer open questions partly because the earlier versions have shown what classes can be used. As soon as there are some countable results the students should make interpretations about the distribution in their own questions and if possible about their correlation to some background variables like age and gender. The next round of discussions means a second look at one’s own answer, feedback to two other students, and suggestions to improve the interview. (For results see [9].)

In the course #4 there are two voluntary research tasks. The first one is a usability test of a security mechanism, typically a program. This is done in pairs, and the reports are evaluated by peer students. This task also deals with IS awareness of the test persons. The second task is to write a 1500-word treatise based on literature. This is done in a step-wise fashion with several stages of peer evaluation and teacher feedback. The student can obtain an extra credit unit for the course by extending the treatise by experiments or other empirical investigations. The results of both these research tasks are published to the world on the course wiki pages. There has been a third research task as well, but due to the increase in laboratories it was on hold at least during 2014–15. The students had to interview a security professional and write a report, which the peer students were supposed to evaluate. The task also had a small ethical content.

3.5 A combination

As we have seen some aspects of EAHR appear together. This is evident also in ethical hacking, see Table 1 at w3-r2. The next row combines all of EAHR, when the task is to discuss alternative ways of doing the research. The instructions mention that some sort of offensive could be possible at the interviewees' premises or at least towards their gadgets. The students find interesting ways to do such things, and they soon turn to discuss ethics. Even if they think such white-hat hacking would be an efficient way to raise the security awareness, they realize that it would consume quite a lot of resources. And not everybody would like to be the target of this kind of wake-up. To concretize, would you like to be warned against poor management of your valuables by white-hat-pickpockets that return you wallet right after stealing it?

REFERENCES

[1] Makasiranondh, W., Maj, S.P., Veal, D. (2011), Student opinions on their development of non-technical skills in IT education, *Mod. Appl. Sci. 5*(2), 3-10.

[2] Rowe, D.C., Lunt, B. M., & Ekstrom, J.J. (2011), The role of cyber-security in information technology education, Proc. SIGITE '11, ACM, 113-121.

[3] Dark, M.J., Epstein, R., Morales, L. et al. (2006), A framework for information security ethics, Proc. 10th Coll. Inf. Systems Sec. Ed. Adelphi, MD. 109-115.

[4] Othmane, L.B., Weffers, H., Ranchal, P. et al. (2013), A Case for Societal Digital Security Culture, IFIP AICT Vol. 405, 391-404.

[5] Albrechtsen, E. (2007), A qualitative study of users' view on information security, *Computers & Security, 26*(4), 276-289.

[6] Trabelsi, Z., Ibrahim, W. (2013), Teaching ethical hacking in information security curriculum: A case study, Global Eng. Educ. Conf. 2013 IEEE, 130-137.

[7] Koskinen, J.A., Kelo, T.O. (2009), Pure e-learning course in information security, Proc. 2nd Int. Conf. Security of Inf. and Netw. ACM, NY, 8-13.

[8] Du, W. (2011), A collection of all 28 SEED Labs, Available at http://www.cis.syr.edu/~wedu/seed/Labs/SEED_Book_1_2011.pdf

[9] Koskinen J.A. (2015), Surveys of daily information security of citizens in Finland, Submitted to IEEE-TrustCom-15.