Specialist Studies in Learning and Teaching

Interactive Learning and Training System for Information Security

Stefan Schumacher

2014-12-20

1 Abstract

This paper was written for the module *Specialist Studies in Learning and Teaching*.
Word count (whole PDF file): 3$\dot{8}$95
The implemented learning object ILTIS can be found at:

- `http://www.bildungswissenschaft.info/ARU3-ILTIS/index.html` or
- `http://www-e.uni-magdeburg.de/steschum/ARU3-ILTIS/index.html`

2 Introduction of the Learning Object

The learning object of my project is IT security in the broadest sense. Due to the time constraints of the seminar I have to narrow it down to one particular task (secure passwords in this case). But I would like to reflect upon the intended interactive learning system as a whole, since I plan on writing my Master's thesis about it and fully develop it afterwards.

IT security becomes more and more important in these days, since IT is becoming more common. According to a survey[1] by the German lobby association for IT companies, more than 75% of German households have internet access. And more than 61% of German professionals use computers at their work place - sometimes even in professions were computers aren't expected, such as plumbing, car mechatronics or maintenance of air conditioning systems.

IT has been introduced into new fields in the industry, such as smart homes, digital companions, business to business relationships or as control mechanisms in modern cars.

[1] `http://www.bitkom.org/de/markt_statistik/64003.aspx` as of 2014-12-06

A new Volkswagen Golf is run by computers in the so called drive by wire technology. There is no longer a bowden control cable running from the gas pedal to the injection pump. Instead there is a multiphase motor at the pedal transforming the pressure into electrical signal transfered by wire to a control circuit at the injection pump. This brings a lot of advantages, like modern safety systems (ABS, ESP etc.) but also some problems like IT security.

Another revolution currently taking place is the spreading of mobile devices – smartphones and tablets – in the personal life of many people. This leads to a situation were more and more information technology is used in a professional context and everydays life, but most people have no idea how information technology works – and therefore now idea how IT security works. Unfortunately, many people store sensitive data on these devices without being aware that there might be security issues. A recent example is The Fappening[2], where several Apple iCloud accounts of actors were cracked and private photos – including nudes – were published.

But even large companies lack a working IT security strategy, with the Sony Playstation Network attack being a prominent example[3]. Intruders gained privileged access to internal Sony servers and could get hold of the data of at least 2.2 million credit cards. And it is not impossible that the intruders got hold of all 77 million data sets[4].

From my own perspective as an IT security consultant I see that a lot of companies have no IT security strategy. Those who do have one often just have a technical strategy, where IT experts (often engineers and computer scientists) think about technical problems. The often ignore the social field of IT security and especially the training of the users. And if a training is done, it is often not done in a pedagogical professional sense but rather using simple methods like handing out some flyers or giving a short frontal instruction on do's and dont's. Without acknowledging all the insights educational science and industrial and organisation psychology gained in the last 80 years.

In my Bachelor's thesis in educational science and psychology I discussed IT security as a topic of education and training and why and how pedagogues come into play. After an extensive search of literature I found no scientific sound – and empirically validated – didactical models of how to reach security awareness in a workforce and how to train them effectively to achieve security aware/competent behaviour.

2.1 Intended Audience

The strategic objective of the project is to develop an interactive training system for IT security. Several modules shall be available for different intended audiences teaching tailor-made subjects. Since this is a too broad (and deep) topic for this modul, I will limit my project to the subtopic of secure passwords.

[2] `http://www.theguardian.com/technology/2014/sep/01/naked-celebrity-hack-icloud-backup-jennifer-law` as of 2014-12-06

[3] `http://www.bbc.co.uk/news/technology-13192359` as of 2014-12-06

[4] `http://www.pcworld.com/article/226775/PlayStation_Network_Users_Reporting_Credit_Card_Fraud.html` as of 2014-12-06

I chose this topic since it affects everyone who uses a computer, it is not too complex like eg. cryptography and it can be taught in an effective way.

The final project will be the implementation of an Interactive Learning and Training System for Information Security (ILTIS[5]).

Due to the complexity of the topic I will create several roles of learners according to their use of IT and/or profession. Some of these role will be end user (the lowest one), system administrator, developer/programmer, information security officer, computer science student, electrical engineering student, mechatronical engineer and others. The intention of this is to create a decision tree that already includes all the relevant subtopics one needs to fulfill the specified role in a company. This is usually done in Germany when new vocations are created or older ones are modernised or deprecated. The German TVET system offers well designed curricula for every recognised vocation which are in the rank of a federal law. This means that every TVET school in Germany has to teach in accordance to the curriculums which in turn leads to a well designed and established system of differentiated vocations. Everyone can easily check what an electrician, carpenter or bank clerk has to know by looking it up in the curriculum. So the complexity of chosing what a learner has to learn has been taken away from the learner. This system will also help to sell the project to companies by offering different bundles with different fees.

In this seminar's subtopic of secure passwords the intended audience is basically everyone who uses a computer or uses some form of login credentials eg. at university or for an email account. Since I cannot estimate the already existing background knowledge of every user, the subtopic has to start at the very beginning[6].

The content of the subtopic will be modeled in the German concept of *professional action competence*. This model breaks down typical processes in a vocation, the professional action fields, into different fields, the learning fields. The learning fields again are broken down by the teacher(s) into learning situations in which the pupils will learn self-regulated. This gives the teachers in TVET schools some freedom about how and what they want to teach at a certain level of detail. It also forces them to create learning situations that are common in the everyday life of a professional in this vocational field, avoiding theoretical teacher centred instructions teaching outdated data[7].

The concept of professional action fields, learning fields and learning situations goes hand in hand with the competency model as described by the Kultusministerkonferenz[8]. The competency model evolved from the now outdated key competence model, which could not solve the vintage problem, the phenomenon that certain knowledge deprecates

[5]Iltis is the German name of the European polecat or mustela putorius and the German name of the project also keeps these initials

[6]My experience as a teacher in the 50+ study programme for students over the age of 50 supports this idea. A lot of those attending by course on IT security don't even know why there are user accounts and credentials in an operating system

[7]`http://enter.educagri.fr/fileadmin/user_upload/pages/Resources_study_days_Codoba/s1_Learning_field_concept_Brauer.pdf` as of 2014-12-06

[8]Standing Conference of the Ministers of Education and Cultural Affairs of the Länder in the Federal Republic of Germany, the body that decides about the rules and standards in the German TVET system

over time. The competency model is action oriented in the sense that it measures performance in a situation, not some form of input (curriculum, learning opjectives etc.). It also accounts for the different psychological factors like motivation when it is used to create assessments(Niegemann et al., 2003; Zumbach and Mandel, 2008; Erpenbeck and Sauter, 2007; Erpenbeck and von Rosenstiel, 2007; Gessler, 2006; North and Reinhardt, 2005).

In my Bachelor's thesis I developed the so called *Sicherheitskompetenz* (security competence), where I used the described competency model and linked it to IT security aware behaviour. This model was developed to allow the creation of more complex learning and teaching situations and systems like the one developed here (**IS:Schumacher:Cyberfrieden**; **mjs:Schumacher:ITWeiterbildung**; cf. Schumacher, 2011).

Since the subtopic of secure passwords is not as complex as cryptography and encrypted emails, the learning situation will be rather simple.

3 Interactive Learning and Training System for Information Security

The Interactive Learning and Training System for Information Security (henceforth known as ILTIS) will contain different learning fields in it's final form. There has to be done more research on the development of the curriculum, but the topics will definitely include following learning fields (ordered by complexity)

1. Tutorial: how to use ILTIS
2. how computers work - Turing machine, layer model, von-Neumann-Architecture, access rights in the operating system
3. how malware works - viruses, worms and trojans
4. secure passwords
5. how encryption works
    a) message digests/hashes
    b) symmetric encryption
    c) asymmetric encryption
        i. mode of operation
        ii. which algorithms do exist?
        iii. how to chose the correct algorithm
        iv. digital signatures
        v. asymmetric encryption of files
        vi. run time and costs of computation

6. how to do backups
7. secure programming
8. how to implement cryptographic programs

The subtopic implemented for this seminar will include a small tutorial on how to use the system and the following subsubtopics:

1. Table of Contents
2. Learning Outcomes
3. Why secure passwords?
4. How to find a strong password
   a) Text based
   b) Videocast
   c) Podcast
5. How to crack a password in less than 5 Minutes (Video)
6. Conclusion
7. Quiz

Every learning field and situation will include a definition of the learning outcomes to make sure the learner knows what he can expect and what is expected of him to know once he finished the field.

To motivate the learner and to explain why he has to gain knowledge of this subtopic I will explain why secure passwords are important. This is important to keep the motivation of the learner up and to enable him of getting mor insight into the learning field. It is often necessary for a learner to make decisions in new situations that differ from the learning situation in a »clean lab setting«(cf. Sekretariat der Kultusministerkonferenz, 2007; Landesinstitut für Schule und Medien Berlin-Brandenburg, 2007; Bader, 2003).

4 Included Media

The media included in the implemented subset of ILTIS is text, images, audio (podcast) and video (screencast, combining a visual presentation and spoken explanation). Every chapter can be finished when a quiz is passed.

I used the definition of meaningful learning by Mayer and Moreno (2003, p 43) defines »meaningful learning as deep understanding of the material, which includes attending to important aspects of the presented material, mentally organizing it into a coherent cognitive structure, and integrating it with relevant existing knowledge. Meaningful learning

is reflected in the ability to apply what was taught to new situations, so we measure learning outcomes by using problem-solving transfer tests« as a base for the learning object. This definition is in accordance with the German model of competency development, though the German literature offers a better way to create a learning product with the teaching methods available in the respective subject didactics (*Fachdidaktik*).

However, Mayer and Moreno (2003) explored the fundamental principle of learning and cognitive load, so his paper gives a lot of insight into how an e-learning environment should be designed. Especially the ideas of his selecting–organizing–integrating theory play a vital role in designing e-learning.

So a main task in the development of the project was to reduce the complexity for the learner by pre-selecting the learning content and editing it in a way to reduce the cognitive load. This was mostly done by breaking the content down into several modules and chapters and by using different media. Pure text may be considered to be old fashioned, but it is beyond question the best known and most used learning method since the creation of schools. So everyone in the target group is able to read and used to learning by instructional texts.

Additional images are used to illustrate complex coherencies. Furthermore I use a podcast and a videocast to explain the contents. A videocast enables the use of images or video sequences to illustrate complex systems. A podcast does not offer this ability, but it is a great method to offer mobile learning units. Mobile learning requires a slightly different approach. Learning units have to be smaller and shorter, since mobile learning often occurs during breaks or the learner has some time to kill eg. while commuting via train to work. So the learning object has to be broken down into smaller parts that are also simpler, since the environment for m-learning is often not as quite and organised as that for e-learning. However, it is a useful method that can be integrated in the grand scheme of teaching eg. for a review unit.

For the not already implemented part I would like to explore the use of games and simulations to use more interactive modules. Several parts of the future curriculum could easily by implemented using a simulation in Flash or HTML5. Simulations work well in explaining technical relationships and how certain principles work. One example could be the use of simulations to explain several forms of encryption.

Especially older cryptographic methods like the Rot13 algorithm used by Caesar in ancient Rome or the Scytale could be easily simulated. This helps the user to develop a basic understanding of how cryptography works. Further cryptographic devices could then be introduced according to their complexity. An interesting example that already exists is `http://enigmaco.de/_fs/index-enigma.html`, a website simulating the German Enigma machine. The shown simulation is beautiful and easy to understand if you understand how the Enigma works. For beginners a simulation would have to be developed that shows the mechanisms of Enigma step by step. This reduces the complexity for the learner and enables him to construct a mental representation of the machine by understanding the principles and building up a mental concept of the atomic operations used.

Games and Gamification can be used to offer rewards that enhance the learning motivation, as shown by neuro scientists (Spitzer, 2006, p. 153) and psychologists (Pollmann,

2008, pp. 258).

Another interactive element that cannot be achieved using traditional media are instructional and interactive videos. The final ILTIS will include at least one module dealing with so called social engineering. Social engineering in the context of IT security describes psychological manipulation of users to gain access to computer systems or to elicit passwords and other secrets from them. Phishing mails and fake websites are a widespread form of this (cf. Schumacher, 2009; Schumacher, 2010).

However, since social engineering works in a social dimension by manipulating human behaviour, reading a text will not help much. Instead I would like to create small videos with typical social engineering situations that are later explained to the audience.

I would also like to add a more interactive element by implementing a kind of point and click adventure in the style of Police Quest or Monkey Island. These computer games have an massive immersive effect and especially Police Quest is a great way to learn about the professional behaviour of a police man in the US[9]. Since the immersive effect of games like Police Quest is huge, they can better be used to train people's behaviour than a simple text. A video or graphical representation in a video is also better suited to explain the tricks and manipulations used in the manipulation of social engineering.

5 Project Management and Life Cycle

I have been working as a software developer for more than 12 years and worked in different larger projects. One of the projects was to create a content management system for a new scientific dictionary, were I developed some web based services (HTML/JavaScript GUI) backed by a database. Other projects I worked in a large open source projects with hundreds of developers living all over the world.

So from a *technical* point of view (maybe software engineering would fit to describe this) I did not learn much from this seminar. My toolchain to develop the project already existed and has been constantly improved since 1997, so the seminar did not add much to it and I could easily implement ILTIS with my already acquired tools, methods and knowledge.

However, keeping in mind that I worked as a software developer for more than 12 years it is understandable that the seminar could not teach me much more knowledge and skills. Pretty much none university seminar could do this nowadays.

However, one thing that worries me about the other students in the seminar is the lack of technical background given. Some of the tools shown allow them to create their own small projects but as soon as the projects grow bigger, other problems will arise. I would like to see more reflection on the limitations of computers and computer programmes on the one hand and learning and the brain on the other hand.

Computer programs suffer from severe limitations of computers being Turing machines, which also limits their ability with regard to being used as a teaching system. It would be greate to discuss this problem, though probably not in the pure mathematical

[9]For an example of PQ watch the playthrough video at `https://www.youtube.com/watch?v=8faVuYZbE4s`

ways of David Hilbert, Alan Turing or Alonzo Church (cf. Turing, 1950; Weizenbaum, 2003; Weizenbaum, 1976).

Another problem that might arise in larger projects is the communication between educational scientists and programmers/computer scientists. It is quite common for computer scientists to work as developers or programmes in projects where the design has to be made in cooperation with other experts. This requires them often to have a profound knowledge of the field they are currently working in. To reflect this development several study courses like computer science in engineering (Ingenieurinformatik) or business informatics (Wirtschaftsinformatik) were established in Germany. Those courses are very succesfull, since they allow the graduates to study an application-oriented minor, which allows them to better understand that field and work together with these experts.

Every serious computer science course also includes seminars on requirements engineering and software engineering. These seminars are used to teach how to manage the software development process and the underlying requirements. It is basically the architectural point of view in computer science, so to speak. Skills and knowledge in this field is vital if computer scientists have to work together with other experts (cf. Dumke, 2003).

So it might also be a good idea to include at least a bit of this knowledge into the seminar. It will massively help those who will go into the field of eLearning.

Regarding the life cycle, I have never been a huge fan of off the rack solutions. There are several content management systems and open learnig platforms available, like Typo3, Wordpress, Moodle or OpenCourseWare.

6 Conclusion

The learning goals defined in the seminar have been mostly met. I am still interested in using small games or gamification in the final ILTIS, but that is probably to complex to be included in the seminar.

I enjoyed seeing the British/American apporach to e-learning, as it differs somewhat from the German approach. However, being still in the German mindset of analysing a problem thoroughly I find the lack of fundamental research in the literature a bit surprising. Psychologist – especially in pedagogical psychology – have done a lot of research about learning and learning settings that seems to be ignored by researchers coming from a media or communications background. And by companies/start ups that are more interested in marketing and getting bought by a big player like Google or Facebook.

A more critical review of the options of e-learning would be a good idea, not only in the underlying psychological fields but also with regards to privacy or simple financial interests of companies involved in e-learning solutions.

However, designing a successful modern e-learning environment is a huge task requiring both – profound expertise in education, training and didactics and in computer science. This has to be brought together in project teams with experts from all fields involved.

References

Bader, R. (2003), 'Lernfelder konstruieren Lernsituationen entwickeln, Eine Handreichung zur Erarbeitung didaktischer Jahresplanungen für die Berufsschule', *Die Berufsbildende Schule* 55 (7/8), pp. 210–217, ISSN: 0005-951X.

Dumke, R. (2003), *Software Engineering:* Vieweg, ISBN: 9783528353551.

Erpenbeck, J. and Sauter, W. (2007), *Kompetenzentwicklung im Netz, New Blended Learning mit Web 2.0*, 1st ed., Luchterhand (Hermann), ISBN: 3472070897.

Erpenbeck, J. and L. von Rosenstiel, eds. (2007), *Handbuch Kompetenzmessung, Erkennen, verstehen und bewerten von Kompetenzen in der betrieblichen, pädagogischen und psychologischen Praxis*, 2., überarb. und erw. Aufl., Stuttgart: Schäffer-Poeschel, XLVI, 796, ISBN: 978-3-7910-2477-6.

Gessler, M. (2006), 'Das Kompetenzmodell', *Handbuch Personalentwicklung – Die Praxis der Personalbildung, Personalförderung und Arbeitsstrukturierung*, ed. by R. Bröckermann and M. Müller-Vorbrüggen, 1. Ausgabe, Stuttgart: Schäffer-Poeschel Verlag, pp. 23–42, ISBN: 978-3791024356.

Landesinstitut für Schule und Medien Berlin-Brandenburg, ed. (2007), *Kompetenzraster im Mathematikunterricht der Grundschule*.

Mayer, R.E. and Moreno, R. (Mar. 2003), 'Nine Ways to Reduce Cognitive Load in Multimedia Learning', *Educational Psychologist* 38 (1), pp. 43–52, DOI: 10.1207/s15326985ep3801_6.

Niegemann, H.M., Hessel, S., Hochscheid-Mauel, D., Aslanski, K., Deimann, M. and Kreuzberger, G. (2003), *Kompendium E-learning*, 1st ed., Springer, 411 pp., ISBN: 9783540438168.

North, K. and Reinhardt, K. (2005), *Kompetenzmanagement in der Praxis – Mitarbeiterkompetenzen systematisch identifizieren, nutzen und entwickeln*, 1st ed., Wiesbaden: Gabler, 221 pp., ISBN: 978-3409143165.

Pollmann, S. (2008), *Allgemeine Psychologie*, 1st ed., München: UTB Reinhardt, ISBN: 3825283917.

Schumacher, S. (2009), 'Psychologische Grundlagen des Social-Engineering', *Proceedings des GUUG Frühjahrsfachgespräches 2009* (Hochschule Karlsruhe), ed. by German Unix User Group, Berlin: Lehmanns Media, pp. 77–98, ISBN: 978-3-86541-322-2.

Schumacher, S. (2010), 'Psychologische Grundlagen des Social-Engineering', *Die Datenschleuder, Das wissenschaftliche Fachblatt für den Datenreisenden* #94, ed. by Chaos Computer Club, pp. 52–59, ISSN: 0930-1054.

Schumacher, S. (2011), 'Sicherheit messen, Eine Operationalisierung als latentes soziales Konstrukt', *Die sicherheitspolitische Streitkultur in der Bundesrepublik Deutschland,*

Beiträge zum 1. akademischen Nachwuchsförderpreis Goldene Eule des Bundesverbandes Sicherheitspolitik an Hochschulen (BSH), ed. by S. Adorf, J.-F. Schaffeld and D. Schössler, Magdeburg: Meine Verlag, pp. 1–38, ISBN: 9783941305311.

Sekretariat der Kultusministerkonferenz, ed. (2007), *Handreichung für die Erarbeitung von Rahmenlehrplänen der Kultusministerkonferenz für den berufsbezogenen Unterricht in der Berufsschule und ihre Abstimmung mit Ausbildungsordnungen des Bundes für anerkannte Ausbildungsberufe*.

Spitzer, M. (2006), *Lernen: Gehirnforschung und die Schule des Lebens*, 6th ed., Heidelberg: Spektrum Akademischer Verlag, 512 pp., ISBN: 978-3827417237.

Turing, A. (1950), 'Computing Machinery and Intelligence', *Mind* LIX (236), pp. 433–460, DOI: 10.1093/mind/LIX.236.433, eprint: http://mind.oxfordjournals.org/content/LIX/236/433.full.pdf+html.

Weizenbaum, J. (Mar. 1976), *Computer Power and Human Reason: From Judgement to Calculation*, W.H. Freeman & Company.

Weizenbaum, J. (2003), *Die Macht der Computer und die Ohnmacht der Vernunft*, 17th ed., Frankfurt: Suhrkamp, 368 pp., ISBN: 978-3518278741.

Zumbach, J. and H. Mandel, eds. (2008), *Pädagogische Psychologie in Theorie und Praxis*, 1st ed., Göttingen: Hogrefe, 353 pp., ISBN: 978-3-8017-2014-8.