Designing and Implementing a CSCL-based Course on the Data Security of a Wireless Learning Environment

Hanna Vuojärvi, University of Lapland, Finland
Hannakaisa Isomäki, University of Jyväskylä, Finland

Abstract

This article reports on a design-based research (DBR) process for designing and implementing a computer-supported collaborative learning (CSCL) course on the data security of wireless learning environments. The study focuses on examining how university students practice data security when learning on a wireless campus, how data security aspects appear in this study and how students perceive the role of data security in CSCL. The research subjects included six pilot students and eight students enrolled in the course. To promote the reliability of the findings, various kinds of data were used. The data was analysed following the grounded theory approach. The results suggest that data security should be considered an integral part of CSCL-based courses and that students need to be taught the basics of managing the data security of their information and communication technology (ICT) enhanced learning environment regardless of the main subject of their studies.

Keywords

Design-based research, Computer-supported collaborative learning, Data security, Higher education.

Introduction

At present, wireless technologies are increasingly used as promoters of flexible eLearning practices. The mobility of technological devices facilitated by wireless technologies gives educational institutions, such as universities, new opportunities to design the use of their pedagogical environments. In this redesign of pedagogical spaces, it is essential to prepare students for the implementation of new learning practices utilising wireless technology. In order to study in wireless virtual communities, students must be able to trust the mediating technologies. This requires increasing students' awareness of data security, particularly because the potential insecurity of Wireless Local Area Networks (WLANs) has been criticised quite heavily in recent years (Furnell & Ghita, 2006). Further, as universities continue to organise their pedagogical practices to support a virtual presence on wireless campuses, the demands for data security, privacy protection and usability of mobile technologies should also be a focus (Isomäki, Päykkönen, & Räisänen, 2008).

This article reports on a design-based research (DBR) process for designing and implementing a computer-supported collaborative learning (CSCL) based course on the data security of wireless learning environments at the University of Lapland. DBR aims to improve educational practices through cycles that consist of analysis, design, development and implementation. All activities are based on tight collaboration between researchers and practitioners (Barab & Squire, 2004; Brown, 1992; Wang & Hannafin, 2005). A special feature of the process presented in this paper was that it took place at the university's wireless campus where all enrolling students had an opportunity to acquire a laptop computer through the university from 2004 to 2009 (Räisänen, Lehtonen, Ruokamo, & Isomäki, 2005). In practice, the university covered approximately two thirds of a laptop's total cost, and the student paid the rest. The laptops included an open-source office-software package, firewall and virus protection and statistical-analysis software. Arts students also had specific software they required during their studies pre-installed on their laptops. Furthermore, a WLAN covering all university premises was launched on the campus. This meant that all students that participated in the course had similar mobile tools and were able to benefit from the mobility afforded by them.

During the first stage of the DBR process, a course on the data security of wireless learning environments was designed and piloted by four teachers. The aim of the first stage was to (a) gather knowledge of current research on data security in academic environments, (b) arrange a pilot course on the data security of wireless learning environments and (c) use the experiences gathered during the pilot course in the *Data Security of Wireless Learning Environments* course design. During the second stage, the *Data Security of Wireless Learning Environments* course was implemented as a part of Information Technology subject studies and Media Education advanced studies. The first aim was to examine the role of data security in CSCL on a wireless campus, the manner in which university students sought to achieve and maintain data security and the manner in which data-security aspects were manifested in this study, while the second aim was to use the research results in refining the course.

The data for this study was collected during the DBR process and consisted of asynchronous network-based discussions students participated in during the course, user diaries that they wrote during and one month after the course and their feedback from the pilot course. The data was analysed using the grounded theory approach (Corbin, 1997).

This article is organised as follows: First, background and previous research are discussed. Then, a presentation of the design framework and research questions is given. Next, a description of the research methods is provided, and the results are presented and examined. Finally, conclusions are drawn and discussed.

Data Security in Higher Education

Information and communication technologies (ICTs) are an integral part of universities' everyday administrative operations, especially in the areas of teaching, learning and research. Increasingly, the ICTs in pedagogical use are mobile, such as in this case laptop computers and wireless networks, as it has been acknowledged that the mobility afforded by mobile tools offers flexibility in learning processes (Demb, Erickson, & Hawkins-Wilding, 2004; Moody & Schmidt, 2004). Mobility is here understood as a wider concept describing not only the mobility of tools but also students' physical mobility, mobility in social and conceptual space, and thus learning is dispersed in time. This promotes students' engagement in their learning and helps them to organise learning activities in a more convenient manner

(Sharples, Arnedillo-Sánchez, Milrad, & Vavoula, 2009.) As the pedagogical use of mobile ICTs develops, it is not only pedagogical decisions that influence the fluency and effectiveness of the teaching and learning processes; technological aspects, such as data security, are also significant.

The data security of academic environments was addressed in a recent research study by querying university staff's perceptions of data security (Drevin, Kruder, & Steyn, 2007) and attempting to determine how to prevent students from cheating on electronic tests (Graf, 2002). It has been outlined that carrying out network-based learning demands paying particular attention to authentication and accountability, access control, intrusion detection, protection of network communications and non-repudiation issues (Furnell et al., 1998). In addition, the viewpoint of end-users on online learning has been emphasised (Furnell & Karweni, 2001). Data security education has been developed concerning both contents and pedagogical practices, but it has mainly been aimed at either the staff of the university (Rezgui & Marks, 2008) or students who are majoring in information systems (Sharma & Sefchek, 2007). The development of data-security practices should, however, be widened to concern all university students, since it has been discovered that putting data-security software into use is one critical part of the domestication process university students undergo when starting their studies on a wireless campus (Vuojärvi, Isomäki, & Hynes, 2010).

The continuously increasing use of mobile ICTs in teaching and learning processes compels researchers to re-examine data security and its role in education. Traditionally, the nature of universities' operations has required public openness, but that should be balanced with data security. Personal laptops enable flexible learning activities, but students must also be responsible for their maintenance, including taking care of data security. From the organisation's point of view, this creates a need to ensure that students are aware of data-security risks and realise that they are key actors in maintaining not only their own but also the organisation's data security. From the students' point of view, data security also potentially affects the learning processes that take place in CSCL communities. Ideally, in CSCL-based courses, students actively participate in collaboration by interacting, sharing experiences and completing tasks together (Jonassen, Lee, Yang, & Laffey, 2005; Stahl, Koschmann, & Suthers, 2006). Reaching a level of productive interaction requires a safe

emotional environment; students need to feel accepted by their peers—to feel trust, respect, belonging and a sense of community (Allan & Lewis, 2006; McInnerney & Roberts, 2004). One way to promote this could be enriching users' awareness of and ability to manage the data security of their CSCL environment. If students trust that data-security solutions are working properly and know how to manage personal data security themselves, they can concentrate on learning without feeling the need to "hold back" just in case their data security might be compromised.

Recent research on information-security training in academia has been approached from various viewpoints of traditional pedagogy; for example, lab-based courses (Jensen, Cline, & Guynes, 2006), seminar-style teaching in classrooms, topic presentations and discussions and course projects for promoting hands-on learning (Li, Zhao, & Shi, 2009). Currently, research concerning university students' perceptions of the data security of their mobile CSCL environment is virtually non-existent. Moreover, most information-security research tends to focus on the technical context (Siponen & Oinas-Kukkonen, 2007). This can be considered a critical deficiency, because students are a significant group of users that use university ICT services every day, possibly with devices that are not organisationally maintained. It is often suggested that the members of organisations constitute a major data-security threat to those organisations (Furnell, 2008; Leach, 2003; Schultz, 2008). In an academic environment, this includes not only the staff but also the students. At a minimum, all users should have the ability to protect their computers against malicious software or other attacks with anti-virus and firewall programs and to control access to their computer or user account. Moreover, successfully implemented data-security solutions have the potential to bring about feelings of belonging and safety, thus supporting the forming of a secure community, which is seen as a critical feature promoting learning in computer-supported communities (Chapel, 2008; Jones & Issroff, 2005; Moody & Schmidt, 2004; Wegerif, 1998).

Design Framework

Course Design

The study reported in this article was conducted as a DBR process that generally aimed to improve educational practices and theoretical constructs through iterative stages of design, implementation, analysis and refinement (Brown, 1992; Cobb, Confrey, diSessa, Lehrer, &

Schauble, 2003; Design-Based Research Collective, 2003). It was based on a tight connection between theory and practice, in that all activities in the process were based on collaboration between researchers and practitioners (Collins, Joseph, & Bielaczyc, 2004; Edelson, 2002; Wang & Hannafin, 2005). Here, this was realised, in that the teachers on the course implementations were also the researchers who analysed the data and refined the course design. This tight connection between research and practice helped to fulfill DBR's dual goal. Firstly, it aims at producing new theories, artefacts and practices that may have an impact on learning. Secondly, it aims at examining these theories and investigating the changes they bring in on a local level. This dual goal brings DBR very close to a kind of learning that takes place in real-life naturalistic settings (Barab & Squire, 2004) such as the wireless university campus in this study.

The first stage of the DBR process involved designing a pilot course based on literature and previous research conducted in the areas of information security, human-computer interaction (HCI) and CSCL. This was done in collaboration between four teacher-researchers. The second stage of the DBR process—implementation of the pilot course—took place in October–November 2006. There were six pilot students, all of them female and aged between 20 and 26 years. They were majoring in either Media Education or Education.

The pilot course started with an introductory lecture that dealt with users' basic security actions, such as users' responsibilities of maintaining the organisation's data security, technical data security risks and protection from these risks. The second lecture concentrated on possible security issues with organising CSCL-type courses. The third lecture was an introduction to data security in wireless networks, and it concentrated on the technical hardware of wireless networks and data security. The fourth and final lecture focused on data security, law and informatics issues and user interfaces.

Between the lectures, students engaged in asynchronous network-based discussions in the Optima environment. After each lecture, students were given a discussion topic that was formulated as follows: (a) Have you used any data-security software? How self-explanatory was it? (b) Form a shared view about data security's role in CSCL-based education. (c) What is your perception of the security level of wireless networks? What kinds of problems or risks

do wireless networks bring about in using learning environments? and (d) How are usability criteria realised in the learning environment that you are using? As their course assignment, students wrote user diaries during and after the pilot course. In the diaries, they reflected on the topics of the lectures and discussions and deliberated on the role of data security in their learning as well as in other areas of life. They also described situations in which they encountered data-security problems and described how they managed those situations. After the pilot course, the students gave anonymous feedback through a learning-management system.

In the third stage of the DBR process, two of the teacher-researchers continued the work by designing the CSCL course on the data security of wireless learning environments. This was done by refining the original pilot course design based on pilot students and teachers' experiences.

Course Description

The course designed based on the pilot course experiences was entitled *Data Security of Wireless Learning Environments*. It was primarily aimed at media education undergraduates and students studying information technology as a secondary subject. The students received four ECTS (European Credit Transfer System) credits for completing the course, which was graded from 1 to 5 or fail. The goal of the course was that the students learn (1) to understand the meaning of data security in CSCL and (2) skills that enable taking care of data security.

Eight Finnish students (4 female, 4 male) between the ages of 20 and 31 years enrolled in the first course implementation in October–November 2007. The students were Media Education, Sociology or Accounting majors. During the seven-week course, students attended thematic lectures, participated in network-based discussions and completed a course assignment. The course started with a lecture that introduced the aims of data security. The second lecture concentrated on data security in practice (i.e., the students were taught skills to maintain data security). This practice-based second lecture was added to the course design on the grounds of students' feedback from the pilot course. According to the pilot students, they would have appreciated more concrete how-to guidance regarding, in particular, virus-protection and firewall software. The third lecture concentrated on security issues in CSCL, and during the

fourth lecture, the students learned about data security in wireless networks, as the lecture concentrated on the technical hardware of wireless networks and data security. The fifth and final lecture covered data security as well as law and informatics issues. The main points of the course were recapped through collaborative mind-map exercises.

Between the lectures, the students engaged in asynchronous network-based discussions in the Optima environment. After every lecture except the first one, they were given a discussion topic that was to be addressed in the discussions. The topics were formulated as follows: (a) Dissect your own computer use in light of the topics presented in the lectures. How do you acknowledge data security in your daily use? (b) Form a shared conception about data security in CSCL. (c) What is your perception of the security level of wireless networks? What kinds of problems or risks do wireless networks bring about in using learning environments? and (d) From a student to the designer of learning environments, what would an ideal and data-secure learning environment be like?

Course assignments were the same as in the first course implementation. Students wrote course diaries and deliberated on the topics handled during the course and their own data-security experiences.

Research Questions

Based on prior research on the topic and the principles of DBR, the research questions of this study were formulated as follows:

1) *What is the role of data security in CSCL on a wireless campus?*
    1.1) *How do university students seek to achieve and maintain data security in CSCL on a wireless campus?*
    1.2) *How are data-security aspects manifested in this study?*
2) *What implications do the results have for the course design and refinement of the course*?

Data-collection and Analysis Methods

Three kinds of data were collected for the analysis. Firstly, there were the network-based discussions that the participating students generated during the pilot and first course implementations. Altogether, there were 139 discussion messages. Secondly, there were 15

learning diaries that the students wrote during and after the course. Both the discussions and diaries were saved in the Optima environment. Thirdly, there was the feedback the students gave anonymously after the pilot course. However, no feedback was available from the first course implementation, because, to ensure students' anonymity, the learning management system through which the feedback was gathered did not allow the teacher to access feedback data if the number of students giving feedback was insufficient.

DBR welcomes the use of various types of data, which helps to achieve data triangulation (Cohen, Manion, & Morrison, 2007). The data was analysed using the grounded theory approach in which the central idea is to develop theoretical ideas and allow relevant issues to emerge from the area of interest; the aim is not to verify an existing theory that suits the goals of the DBR process (Glaser & Strauss, 1967). During the research, the processes of data collection, analysis and interpretation were interwoven (Corbin, 1997; Strauss & Corbin, 1998; Suddaby, 2006). The method included three phases of data coding: open, axial and selective coding. Even though these phases are presented here as individual phases of the analysis, they do not necessarily take place in stages; rather, a researcher may move between coding procedures (Strauss & Corbin, 1998).

Results

The open, axial and selective coding phases of grounded theory analysis and the resulting categories are presented in Figure 1.

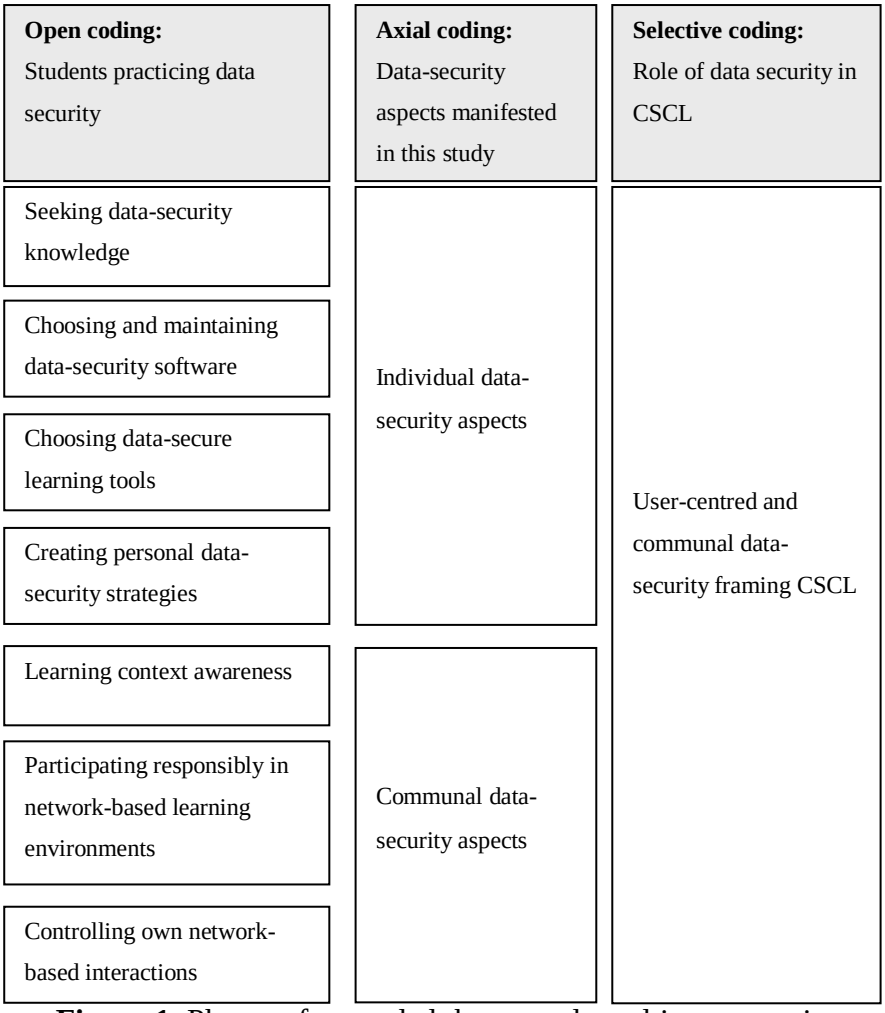

Figure 1. Phases of grounded theory and resulting categories.

The analysis is described in detail in the sections that follow. Empirical evidence is presented by referring to quotations from the discussions, feedback and students' diaries. Students' names have been changed to protect their identity. The justification of the analysis is facilitated by explicating the different levels of data in each phase of the analysis.

Open Coding – Students Practicing Data Security

The first phase—open coding—started by reading through all the diaries, threaded discussions and feedback and identifying concepts relevant to the focus of the study (i.e., the manner in which students seek to achieve and maintain data security in CSCL, the manner in

which data-security aspects are manifested in this study and the role of data security in CSCL). This phase was initiated simultaneously with the discussions, which is typical in grounded theory analysis. The data does not have to be collected in its entirety before the analysis, but the coding can start as soon as some data is collected. The first phase yielded 21 concepts, which were placed into seven categories: (a) seeking data-security knowledge, (b) choosing and maintaining data-security software, (c) choosing data-secure learning tools, (d) creating personal data-security strategies, (e) learning context awareness, (f) participating responsibly in network-based environments and (g) controlling own network-based interactions.

The first category—*seeking knowledge about data security*—was created from four concepts: learning from friends, attending data-security courses, reading IT magazines and learning from the university's help desk personnel. Nearly all the participating students mentioned that they had deliberated upon issues concerning laptops with their friends. The more experienced students had taught the less experienced students about the functionalities and best practices concerning the laptop. Some of them had also attended courses organised by the university, but for most, this was the first ICT course they had attended. In general, the students hoped that there would be more guidance concerning the use of laptops in learning. Some of the students had had help from the university's help desk personnel.

The second category—*choosing and maintaining data-security software*—was created from three concepts: setting up virus-protection software, setting up firewall software and creating software policies. The original laptop configuration included virus-protection and firewall software, but some of the students had changed them before the course started. Changing the software became topical for all students, since a few days before the first course implementation started, the university's ICT services announced that the firewall software that was installed on the students' laptops should be uninstalled, because the campus license would expire. The students were advised to independently choose and install new firewall software on their laptops. This presumably had an effect on the students' deliberations in their diaries and network-based discussions. In general, the students were pleased that it was possible to fit firewall-installation guidance into the course structure.

> *This course was arranged at a convenient time for me. University ICT services had announced that McAfee firewall was to be uninstalled and we had to find new software.* (Edith, diary)

The third category—*choosing data-secure learning tools*—was created from two concepts: selectiveness when loading software from the Internet and choosing proper software. The students seemed to be quite cautious about choosing software. As they had administration rights, they were able to install and uninstall their software of choice on their laptops. They wrote in their diaries and stated during network-based discussions that they did not want to upload anything extra from the Internet—only the software they truly needed and knew how to use. The most often mentioned software applications were Internet browsers and different kinds of office tools such as word processors and presentation graphics software. Data security played an important role, especially when deciding what Internet browser to use.

> *I am quite strict concerning what to allow on my laptop.* (Annie, discussions #4)

The fourth category—*creating personal data-security strategies*—was created from three concepts: managing own personal user identification, managing backup copies and defining access to laptop. Both in their diaries and in network-based discussions, the students deliberated the password issue from multiple standpoints. They all described having several passwords, each for a different kind of system. Topically, a piece of news was reported a few weeks before the course started according to which a long list of user-identification information was stolen and published on the Internet. This raised concerns and discussions among the students about having and storing passwords and possible future identification procedures (e.g., fingerprint technologies). The usual backup forms were copying files to a memory stick, copying files to an external hard drive and copying files to a folder on the university's server. Access to the laptop was controlled through defining usernames and passwords and restricting the availability of user accounts. The necessity of user identification to gain access to network-based services is common to every computer user nowadays, and this was also evidenced by the students' diaries and discussions. It was also a commonly used strategy to restrict the number of user accounts available on their laptops. Most of the students had created only one user account for their own use.

> *To cover my family's needs, I purchased a network hard drive to which it's possible to save files from multiple computers.* […] *I have also used my own folder on the university's server to store my backup files.* (Tom, diary)

The fifth category—*learning context awareness*—was created from three concepts: being aware of private and public spaces, adjusting own behaviour regarding the context and choosing the type of network in view of the activities involved. These three concepts came about when the students deliberated on how to set the boundaries between the private and public physical places where technology is used. Public places, such as the university, are perceived as critical places where all information-security functions must be up and running. Private and public considerations were also in focus when defining private and public network-based activities. According to the students, they did not want to pursue all their activities through wireless networks, because they perceived them as more risky than, for example, an ADSL (asymmetric digital subscriber line) or cable network connection. Having, for example, neighbours' WLAN Internet connections available in the network list in one's home environment was perceived as irritating. The students thoroughly deliberated on the characteristics of wireless and wired networks and the manner in which they might affect the user. In addition to the types of data-security mechanisms, they also thought about access issues.

> *Somehow, I have had an image that a wireless network would be more secure than [a] wired network. Perhaps this image is because wireless is "in the air" and invisible, harder to see.* (Rachel, discussions #34)

> *A laptop is surely as private as a desktop PC, but still, I perceive it [as being] more public. A desktop is always at home, inside four walls, whereas a laptop is with me everywhere among foreign crowds.* (Ally, diary)

The sixth category—*participating responsibly in network-based learning environments*—was created from four concepts: determining access rights to one's own materials, determining access rights to a group's outputs, protecting shared workspaces and taking care of personal

data security in a learning community. Students perceived the network-based learning environment they used during courses as a private area. All the files, discussions and exercises in that environment were meant for the group's eyes only and needed to be protected. They also realised that data-security procedures were there to support their learning processes. From an individual point of view, it was important to know who might read their texts. They identified several types of texts that they produced in network-based learning environments of differing degrees of sensitivity. Some contained more personal information, while others contained more report-type texts that were not highly sensitive. Students felt that through restricting access to documents and essays that included mostly personal deliberations on the subject of the study, they could maintain their privacy and protect their identity.

> *I think that data-security issues should be highlighted before accessing [a] network-based learning environment. At least I haven't had any guidance about data security relating [to] my network-based studies. […] Especially as the laptops are becoming more common, I think that it is everyone's responsibility to get the needed data security on their own computer. In a communal learning environment, responsibility is shared by everyone, as we are working together. So if one of us breaks the rules, everybody suffers.* (Ally, discussions #21)

The seventh and final category—*controlling network-based interactions*—was created from two concepts: being cautious with the use of MSN Messenger and maintaining several email accounts. Many of the students had several email accounts for different purposes. They did not want to share their "official" email address that they had received through the university with unofficial parties. One student had five different email accounts for studying, work, discussion forums, hobbies and e-shopping.

> *Because of trash mail, I have several email accounts. I'll share the not-so-important address for general use and accordingly receive about 20-30 trash mails every day*. (Adam, discussions #3)

The first follow-up question of this study was, *How do university students seek to achieve and maintain data security in CSCL on a wireless campus?* The analysis shows that students are oriented towards embedding data-security practices in their daily routines. This emphasises the importance of organising and developing data-security education for all students in the university, not only those majoring in information systems (e.g., Sharma & Sefchek, 2007). Firstly, it seems that students try to find out about data security and gather knowledge about topical issues. Secondly, they perceive it as important to play an active role in managing data security. Students are quite specific in terms of how they feel software should work, and they are prepared to try out multiple options and make comparisons before choosing. Thirdly, students try to be aware of the context in which they are using their laptops and networks, and they often create personal data-security strategies through which they can manage user-identification information, backup copies and laptop access. Fourthly, students perceive themselves as members of a learning community in which everyone has to assume responsibility for data security.

Axial Coding – Data-security Aspects Manifested in this Study

After the data was broken down in the open coding phase, it was reassembled in the second phase—*axial coding*. This was done by comparing categories in a way that reveals how two or more of them might be linked. During this process, it was noticed that the categories 'Seeking data-security knowledge', 'Choosing and maintaining data-security software', 'Choosing data-secure learning tools' and 'Creating personal data-security strategies' all described how students adjusted the laptop to meet their personal data-security demands. Therefore, the first axial coding category was labelled 'Individual data-security aspects'.

The second axial coding category 'Communal data-security aspects' was formed on the basis of the open coding categories 'Learning context awareness', 'Participating responsibly in network-based learning environments' and 'Controlling own network-based interactions'. Through these three categories, students were able to describe how they sought data security in the CSCL community of which they were a part.

The second follow-up question of this study was, *How are the aspects of data security manifested in this study?* As reported earlier, authentication and accountability, access

control, intrusion detection, protection of network communications and non-repudiation issues are the key data-security aspects that need to be considered when carrying out network-based teaching and learning (Furnell et al., 1998). The analysis revealed that the data-security aspects come about in terms of individual and communal points of view. When thinking about individual aspects, students pay close attention to choosing the right kind of data-security software and data-secure office software. This can be seen as considering authentication and accountability and intrusion detection. Access control came about in creating personal data-security strategies, particularly when defining access to the laptop. In communal aspects, authentication and accountability and access control were regarded as defining who has access to network-based communal learning environments. Protection of network communications was another communal data-security aspect.

Selective coding – Role of data security in CSCL

The third phase of the analysis was selective coding. This phase considered how the three categories that were formed during axial coding could be integrated into one central category. The core category that emerged as a result of selective coding was labelled 'User-centred and communal data-security framing CSCL'. This answered the first research question of this study: *What is the role of data security in CSCL?*

It was noticed that students described how data security, on the one hand, created rules and restrictions for their actions and, on the other hand, worked as a tool that they could use to protect learning outcomes and their privacy. For example, access is controlled on multiple levels. Students are asked for identification information when logging on the system, and inside the system, they have available only the workspaces of those courses in which they are enrolled. Inside one course's workspace, the teacher can restrict access to some information (e.g., between groups). The students were content with the way access control was handled in their network-based learning environment. They perceived it as a closed area that was available only to those participating in the course. This can be understood as their need for a safe place to study, where they could feel they belonged to a certain group while experiencing trust and respect (Allan & Lewis, 2006; McInnerney & Roberts, 2004).

Access issues also came about when the students described how they managed their laptop computers. They perceived very strongly that the laptop was their personal and individual learning tool that created a private space in which they could learn. That is why they wanted to restrict access to their own laptop by, for example, using only one user account protected by a password. Students were also very keen on selecting the tools that they used on their laptops. Office tools, such as word processors and Internet browsers, were selected in terms of usability and data security, which was highlighted especially when the students mentioned their selection of an Internet browser. Having specific data-security software was perceived as essential.

Concretely, the idea of a private learning space came about when students described the places in which they used their laptops. The awareness of private and public places played a very important role in deciding when and where to study. The data security of the WLAN and public spaces such as the university was perceived as weak, and that is why some activities were preferably performed in a home environment. In particular, the inconsistent availability and slowness of the WLAN were perceived as undermining students' perceptions of a secure learning environment.

Data security can also be seen as framing learning when thinking about the level of knowledge of data security that students possess. In their writings, all the students noted that they did not really have a clear idea about data security or possible threats or enough expertise to manage their own laptop and, thus, did not fully utilise their laptop. They mentioned that participating in this course had opened their eyes and given them knowledge they could fall back on when using their laptops.

Implications for Course Refinement

The second main research question of this study was, *What implications do the results have for the design and refinement of the course?* Three particular points need to be addressed in the next stage of the DBR process.

Firstly, students need practical how-to skills, and the course should include practical training sessions. Practical aspects played a larger role in the first course implementation, because the

pilot course feedback clearly indicated a need for that, but their role in course design could be emphasised. It would be beneficial to learn to evaluate different features of software and give reasons based on which tools they choose to use. Secondly, current data-security software needs to be considered when designing the course contents. Some preinstalled software applications are available on the laptop as students get them, and changes will occur in time due to changes in campus licences. This means that the course designers should collaborate more closely with the university's ICT services to gain knowledge about these changes as early as possible. Thirdly, more attention in the course design should be directed to the social aspects of data security. This is an emerging research area, which means that there is no extensive knowledge base on which the course design could be grounded, but students' responsibilities to the community can nevertheless be highlighted.

Conclusions and Discussion

In this article, a DBR process of designing and implementing the *Data Security of Wireless Learning Environments* course was presented. The results of the grounded theory analysis suggest that data-security training should be considered as a part of CSCL-based teaching and learning. The educational use of ICTs involves not only planning pedagogical aspects but also considering the technology and analysing how it can be used in such a manner that it supports students' collaborative actions, problem solving and interaction in a safe community. Generally, students must try out and learn to use their ICT tools in addition to the main subject of the courses in which they enrol. In this case, the main goals of the course were learning about technology and exploring data-security issues in particular, which was perceived as beneficial by students—not only regarding the completion of this particular course but also in terms of their studies in general. Even though today's university students are more computer savvy than those of the past, it seems that they need a deeper understanding of data-security issues in order to be able to consider their computer usage from a security point of view.

Teaching students about data security may have more far-reaching influences than just promoting their learning. Today's work environment relies heavily on information technology: Employees are assumed to have information technology skills, including skills related to data security, to manage their work. Additionally, technological solutions cover

other areas of life as well. Teaching students basic data-security knowledge and skills could very well be considered an opportunity to educate them not just for their degrees but for their future lives as well.

Acknowledgements

The study was conducted as a part of the MobIT research project funded by the Finnish Ministry of Education for the years 2007–2009.

References

Allan, B., & Lewis, D. (2006). The impact of membership of a virtual learning community on individual learning careers and professional identity. *British Journal of Educational Technology, 37*(6), 841–852.

Barab, S., & Squire, K. (2004). Design-based research: Putting a stake in the ground. *Journal of the Learning Sciences, 13*(1), 1–14.

Brown, A. L. (1992). Design experiments: Theoretical and methodological challenges in creating complex interventions in classroom settings. *Journal of the Learning Sciences, 2*(2), 141–178.

Chapel, E. (2008). Mobile technology: The foundation for an engaged and secure campus community. *Journal of Computing in Higher Education, 20*(2), 15–23.

Cobb, P., Confrey, J., diSessa, A., Lehrer, R., & Schauble, L. (2003). Design experiments in educational research. *Educational Researcher, 32*(1), 9–13.

Cohen, L., Manion, L., & Morrison, K. (2007). *Research methods in education*. New York, NY: Routledge.

Collins, A., Joseph, D., & Bielaczyc, K. (2004). Design research: Theoretical and methodological issues. *Journal of the Learning Sciences, 13*(1), 15–42.

Corbin, J. (1997). *Grounded theory in practice*. Thousand Oaks, CA: Sage.

Demb, A., Erickson, D., & Hawkins-Wilding, S. (2004). The laptop alternative: Student reactions and strategic implications. *Computers and Education, 43*(4), 383–401.

Design-Based Research Collective (2003). Design-based research: An emerging paradigm for educational inquiry. *Educational Researcher, 32*(1), 5–8.

Drevin, L., Kruger, H. A., & Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security, 26*(1), 36–43.

Edelson, D. C. (2002). Design research: What we learn when we engage in design. *Journal of the Learning Sciences, 11*(1), 105–121.

Furnell, S. (2008). End-user security culture: A lesson that will never be learnt? *Computer Fraud & Security*, 4, 6–8.

Furnell, S. M., & Ghita, B. (2006). Usability pitfalls in wireless LAN security. *Network Security*, March, 4–8.

Furnell, S. M., Onions, P. D., Knahl, M., Sanders, P. W., Bleimann, U., Gojny, U., & Röder, H. F. (1998). A security framework for online distance learning and training. *Internet Research*, *8*(3), 236–242.

Furnell, S. M., & Karweni, T. (2001). Security issues in online distance learning. *VINE*, 123, 28–35.

Glaser, B., & Strauss, A. (1967). *Discovery of grounded theory*. Chicago, IL: Aldine.

Graf, F. (2002). Providing security for eLearning. *Computers & Graphics*, *26*(2), 355–365.

Isomäki, H., Päykkönen, K., & Räisänen, H. (2008). Secure collaborative learning practices and mobile technology. In G. D. Putnik & M. M. Cunha (Eds.), *Encyclopedia of networked and virtual organizations*, Vol III (pp. 1407–1412). New York, NY: IGI-Global.

Jensen, B. K., Cline, M., & Guynes, C. S. (2006). Teaching the undergraduate CS information security course. *Inroads – The SIGCSE Bulletin*, *38*(2), 61–63.

Jonassen, D., Beng Lee, C., Yang, C.-C., & Laffey, J. (2005). The collaboration principle in multimedia learning. In R. E. Mayer (Ed.), *The Cambridge handbook of multimedia learning* (pp. 247–270). Cambridge, UK: Cambridge University Press.

Jones, A., & Issroff, K. (2005). Learning technologies: Affective and social issues in computer-supported collaborative learning. *Computers & Education*, *44*(4), 395–408.

Leach, J. (2003). Improving user security behaviour. *Computers & Security*, *22*(8), 685–692.

Li, J., Zhao, Y., & Shi. L. (2009). Interactive teaching methods in information security course. *Proceedings of the International Conference on Scalable Computing and Communications* (pp. 489–493). IEEE Computer Society.

McInnerney, J., & Roberts, T. (2004). Online learning: Social interaction and the creation of a sense of community. *Educational Technology & Society*, *7*(3), 73–81.

Moody, L., & Schmidt, G. (2004). Going wireless: The emergence of wireless networks in education. *Journal of Computing Sciences in Colleges*, *19*(4), 151–158.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher-education: An exploratory study. *Computers & Security*, *27*(7–8), 241–253.

Räisänen, H., Lehtonen, M., Ruokamo, H., & Isomäki, H. (2005). Network-based mobile teaching and studying on a wireless campus. In P. Kommers & G. Richards (Eds.), *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications 2005* (pp. 599–604). Chesapeake, VA: AACE.

Schultz, E. (2008). The human factor in security. *Computers & Security, 24*(6a), 425–426.

Sharma, S. K., & Sefchek, J. (2007). Teaching information systems security courses: A hands-on approach. *Computers & Security, 26*(4), 290–299.

Sharples, M., Arnedillo Sánchez, I., Milrad, M., & Vavoula, G. (2009). Mobile learning. In N. Balacheff, S. Ludvigsen, T. de Jong, A. Lazonder, & S. Barnes (Eds.), *Technology-enhanced learning: Principles and products* (pp. 233–249). New York, NY: Springer.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *The DATA BASE for Advances in Information Systems, 38*(1), 60–80.

Stahl, G., Koschmann, T., & Suthers, D. (2006). Computer-supported collaborative learning. A historical perspective. In R. K. Sawyer (Ed.), *Cambridge handbook of the learning sciences* (pp. 409–426). Cambridge, UK: Cambridge University Press.

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research – Techniques and procedures for developing grounded theory.* London: Sage Publications.

Suddaby, R. (2006). From the editors: What grounded theory is not. *Academy of Management Journal, 49*(4), 633–642.

Vuojärvi, H., Isomäki, H., & Hynes, D. (2009). Domestication of a laptop on a wireless campus. *Australasian Journal of Educational Technology, 26*(2), 250–267.

Wang, F., & Hannafin, M. J. (2005). Design-based research and technology-enhanced learning environments. *Educational Technology Research & Development, 53*(4), 5–23.

Wegerif, R. (1998). The social dimensions of asynchronous learning. *Journal of Asynchronous Learning Networks, 2*(1), 34–49.