Portfolio for PGCAP

Hans Georg Schaathun

University of Surrey

Department of Computing

2008

Contents

1. Introduction

This report (hopefully) concludes, for me, PGCAP — Postgraduate Certificate in Academic Practices. The two main parts are a reflective commentary on the full breadth of my professional development in Chapter 2, and a report from the revision of a taught MSc module in Chapter 3. This introduction, and the conclusion in Chapter 4 speak for themselves.

Some readers may find that the format of the report is unconventional, particularly in the referencing style. I follow the norm from my own field of research, which is what I know and what is best supported by my software. Although Harvard style referencing probably is available in LaTeX, learning to use it is non-trivial, and it is hardly relevant for the learning objectives.

1.1. My starting point

When I joined Surrey, I had a very varied background from Academia, including a year primarily teaching, 2-3 years as full-time researcher, and half a year primarily coordinating research proposals. Starting in my first permanent post in February 2006, there were few new tasks. However, even so, the much wider range of *concurrent* responsibilities still made a steep learning curve.

My teaching experience included convening two modules as substitute lecturer. Although both modules were established, both required revision and inclusion of some new material. As a PhD student I was a teaching assistant, which involved contributions to a varied range of modules. In several cases, I had a separate responsibility for preparing exercises and lab work. I also led the one-week crash course to the computer system four times, and completely revised it twice. As a post.doc., I supervised two post-graduate dissertation projects (1 year worth of work over $1\frac{1}{2}$ year).

My doctoral training was exceptionally publication-driven, and from the start of my PhD in 1999 to my arrival at Surrey in 2006, I had published 18 full, refereed papers. This does include six conference papers in *Lecture Notes in Computer Science*, but it also includes six papers in *IEEE Trans. Information Theory* with an Impact Factor about 2.

I had a significant international network, including co-authors at seven different institutions in five different countries. I had also had a nine-month research stay at ENST, Paris, and a six-month stay at Royal Holloway.

Joining Surrey as an academic, very few tasks were new. The main challenges became organising my time to cope with the wide range of *parallel* tasks, and to find my way through the people and the administrative and academic routines in a new environment. By department policy, many tasks (such as second examiner, placement visits, etc.) are

distributed evenly on the academics. Although this ensures that everyone is familiar with the full breadth of teaching activities, it is also time consuming as each individual task must be learnt and organised.

There has also been challenges relating to what the discipline of *Computing* is, or should be. I come from a department of Informatics. That is not entirely meaningful, as informatics is a word only rarely used in English. It is most often translated as Computer Science, but the boundaries to related fields like Mathematics and Electronic Engineering tend to be different from country to country, and from institution to institution. My own degrees tended very much towards mathematics.

The Surrey concept of *Computing* is also different from the international concept of *Computer Science*. It has been department policy to make computing a very broad and wide-ranging discipline. The best-selling degrees have had a strong business and management flavour. The result is a large number of project students with very weak programming skills, which many people would consider the very basis of any Computing degree.

1.2. Acknowledgements

I am very grateful for the feedback and discussions with the current PGCAP course leader, Dr. Trevor Welland. Without him, there would have been no direction.

I would also like to thank very helpful colleagues in the department for their support and feedback when I have been tackling new tasks in the job. Particularly Dr. Nikos Antonopoulos and Dr. Matthew Casey are excellent mentors — whether or not it is their formal responsibility — and I have used their help a lot. Head of Department, Prof. Steve Schneider has provided a lot of very useful support, especially on grant proposals. Advice from Dr. Helen Treharne and Dr. Jonathan Clark has also been valuable.

Several friends in the scout movement has over the years, been of great help to me, learning how to approach learners with good questions which provoke thought and inspire further enquiry. In particular, I would like to thank Endre Helland, Kjersti Kvaløy and Knut W. Hansson.

2. Reflective Commentary

2.1. Teaching

During my first two years, I have developed and taught two new modules for the MSc programme in *Security Technologies and Applications* (STA) which started in September 2007:

- CSM25 *Secure Information Hiding* (Steganography) in the Spring Semester, and
- CSM27 *Computer Security* in the Autumn Semester.

Both modules are compulsory for STA. CSM25 was also made available in Spring 2007 as an option for the two existing MSc programmes in *Internet Computing* (IC), and *Information Systems* (IS). In 2008 it was also optional for IC, and for IS students with adequate background (by individual agreement). It has now been decided that CSM27 will become compulsory also for IC from 2008/09.

As I designed the modules, I also chose the assessment form. This started as a hyper-conventional combination of 60% coursework and 40% written exam for CSM25 2007. With increasing experience, I no longer feel the need to be conventional, so the assessment scheme is under development, as will be discussed in the sequel. In short, I'd describe it as a gradual movement towards portfolio-based assessment.

Each module is 15 credits and supposed to have 30-36 contact hours. Following the norm in the department, this has become one 3h session per week. The students are split; some strongly prefer concentrated teaching (to avoid having to come to the university every/all day), while others strongly oppose it (because it is hard to stay focused for 3h). However, I am free to choose the format, both concerning session duration, and also concerning the division between lectures, seminars, tutorials, lab classes, or other teaching and learning fora.

Formal evaluation of the modules are shown in Appendix D and E. The feedback from peer observation is shown in Appendix G. Module descriptions are in Appendix F. The feedback form from senior observation is annexed (due to insufficient IT support in the university, it was not possible to include this in the document proper).

In addition to taught modules, I supervise final year projects (BSc 45 credits), and MSc dissertations (60 credits), and visit two students per year on professional training.

2.1.1. Teaching ethos

A pillar in my teaching methodology is the techniques I have learnt as an adult scout leader [nsf97]. This includes the following four principles:

- Be positive. Never talk about what is bad, but rather about what can be improved. High-light more positive features than things to improve. Typically 3 positive and 1 challenge ($+++\Delta$).
- Continuous evaluation. Give and prompt for feed-back regularly, and use it to improve.
- Use good questions to force the students to think, and to reflect over their own learning.
- Learning by doing. More is learnt through relevant activities than through passive digestions of books and lectures.

Mainly, these principles are supported, using other words, by the expertise on teaching and learning, The case for activity-based learning (learning by doing) is particularly strong, and several studies confirm that activity makes the learning more effective, e.g. [Big03, p. 80].

A main theme in [Big03] is the reflective practitioner. Although he does not explicitly talk about reflective students, that seems to be the essential objective in some of the assessment tools he suggests, such as the portfolio. Good questions is the catalyst for reflection.

The importance of positive feedback is less explicitly emphasised in the PGCAP literature, but the warning against negative feedback was emphasised in [Com07]. The students do not have to be told that their work is bad — most often they know. What they do need to know is *how* to improve. Biggs [Big03] also encourages a view of good performance being the result of *effort* more than inherent *ability*, both for students and for teachers. Hence, feedback should be designed to encourage effort, not identify lack of ability. I think that this is an implicit key point in the use of 3 pluses and a challenge as I am used to.

When I try to restrict myself to 1-2 challenges to work on, it is to prevent the students from spreading to thin. In most cases, a serious effort on one key issue may mean a massive quality improvement, and the student is better off focusing on this and do it properly, rather than trying to fix on minor issues.

I find it very interesting to see the similarities between the scout ethos and the teaching methodology promoted by John Biggs and Andrew Comrie. Although I always tried to apply these principles, I did at the beginning feel restrained by established practice in the department. The literature on education as presented by PGCAP has given me two important things which, together, enable me to use them more consistently in the future. Firstly, the literature increases my confidence in the principles and their applicability to higher education. Secondly, I have found many good ideas on *how* the principles can be, and have been, applied in higher education.

There have been no major challenges in applying the principles just described. It has meant deviating from established customs in the department, but as long as the deviation is introduced gradually, no real opposition has been encountered. It is harder to engage grown-up students than children, because they have a firmer expectation of

the forum and teaching environment, and this is discussed below. The greatest challenge is to design good exercises to support learning by doing, but this is going to remain a challenge any time a module is designed on a new topic.

2.1.2. On the use of questions and interaction

I did receive positive feedback from the teaching observers on some of the methods arising for the ethos described above. My peer partner high-lighted my habit of always, after having attempted to answer a question from the students, to ask whether I had answered it properly.

The senior observer high-lighted the strong rapport I had established with the students in CSM27, and the good atmosphere for discussion, where the student felt confident to ask questions.

A few times, I have asked each student in class about the 'most useful' or 'most important' piece of learning from the last week. In CSM25 this had limited value, and almost all answers were too obvious, superficial, and repetitive. It worked very well when I asked after the weekly exercise in CSM27 (Week 7), and this served as a useful confirmation that the exercise had been effective.

Biggs [Big03, p. 243] reports successful use of similar questions in a portfolio-based course. These questions in themselves may not be sufficient to create the reflective environment needed to answer them, and this probably explains my failure in CSM25. The key to Biggs' success is probably a consistent use of reflective activities throughout the course and leading to the portfolio. My approach in CSM27 is similar, albeit less consistent, where the weekly exercises aim to inspire reflective and critical thought processes.

I had considerably more success with student interaction in CSM27 (Autumn) than in CSM25 (Spring). It is hard confidently to establish the cause, but several hypotheses are reasonable.

- Students with different cultural backgrounds. In CSM25, there were no ethnically British students, and few Europeans. In CSM27 there was a significant number of ethnic Britons, and many more born and bread in this country, as well as a few from the Mediterranean.
- Students at different skill levels. The new STA programme has attracted more first and upper second class students than IS has.
- Better exercise programme in CSM27. As discussed in the project report (Chapter 3), I increased the emphasis on exercises with peer assessment and class discussions in CSM27.

In a sense, it does not matter what the primary cause is. There is not a lot I can do about the first two, and there are enough reasons to continue the emphasis on interactive exercises (Cf. Chapter 3). It is an open question how effective the improved exercise programme will be with the clientele traditionally known from IS, and I will seek an answer the next time I teach such a class.

2.1.3. On the use of learning activities

During my own studies, I have always taken more interest in tutorials over exercises than in regular lectures. Few lecturers teach well enough to give more than reading a book, and I have often done modules without attending lectures at all. The tutorials, being interactive, have on the other hand provided an opportunity qualitatively different from the book, and often given feedback on my own solutions prepared between sessions. I have done much more to attend tutorials than lectures.

When I was planning my first module to teach (CSM25 Spring 2007), I had this combination of lectures and tutorials in mind. Apparently it is not the normal format in the department. The system absolutely depend on students doing exercises between sessions, so that there is something to discuss in the tutorial. Discussing it with senior staff, the emerging viewpoint was that English students do not do exercises between lectures unless they are marked.

Based on this viewpoint, CSM25 was prepared with exercise time in class, but this was never good enough (cf. Chapter 3). The solution adapted in CSM27 Autumn 2007 came from a suggestion by Andrew Comrie [Com07], and also suggested by Biggs [Big03]. An assignment is given every week to be completed at home, and brought to class for peer assessment and discussion. Only a subset of the papers are requested for end-of-term assessment, where the students have the opportunity to revise the paper in view of the peer assessment and of subsequent learning.

When I planned this scheme for CSM27, the intention was to force the students to do exercises every week, by making it clear that there would be insufficient time to make the requested subset from scratch at the end of term. This appears to have worked. Most students did the exercises most of the weeks.

Another advantage of the approach, as reported by Gibbs [Gib], is that students tend to make better papers when only a subset is marked. In his example, the initial scheme assessed 25 reports, each report having only marginal influence on the grade. When it was announced that only four random reports would be marked, each of them would have significant impact on the grade, and the students prepared 25 good reports.

Also in my module, the students clearly made an effort with these papers, with eight distinctions, eight merits, one pass (which was closer to merit than to fail). The only failures were due to plagiarism.

2.1.4. On portfolio evaluation

Portfolio evaluation was one of the great buzz words in higher education policy in Norway at the time I left for Surrey. It was used by politicians, and had little meaning for the academics. To the extent it was understood by lecturers, it was expected to cause an unacceptable increase in workload.

I did agree with the common view. If portfolio evaluation is to be introduced overnight, I still think I was right. However, I now find that it is the basic elements and principles of portfolio evaluation which are interesting, and individual elements can to a large extent be introduced independently.

The system of weekly exercises can be viewed as a first step towards portfolio assessment. In my implementation I already asked for two papers chosen by me and one chosen by the student. This gives the students some limited opportunity to choose their own focus.

In hind-sight I regret that I did not ask for a concluding essay, letting the students tell me what they consider the most important piece of learning from the module. This would have given a number of potential advantages:

- Useful feedback on the module.
- It would prompt the students further to reflect on the material.
- It would save time in the marking, as the conclusion would probably point to the high-lights of the individual papers.

In a further development of the assessment scheme, I would add this essay, and possibly give more flexibility in choosing items to support the conclusion in the essay. There is no strong reason why the chosen items have to be from the weekly exercises, although most students may find it easier to use those. I will still ask for some specific papers, to get a sample of the breadth of the student learning.

I also have to work more on the assessment criteria, and publicise them in advance. Part of the reason this was not done this time around, is that I was unable to predict what the students could do in a week. Now I know more about this, and I am better placed to phrase good criteria next time.

2.1.5. Student evaluation in CSM27

In CSM27 (fourth week), I tried an evaluation exercise suggested by Andrew Comrie [Com07]. The students were asked to post yellow stickers on the wall, under the following three headers:

Alter Things about the teaching which should be changed.

Begin New things (methods or topics) which should be introduced in the teaching.

Continue Good features about the previous teaching which should continue.

A complete list of the outcome is included in Appendix A. Below I will discuss the comments which stood out as most important, either because they were repeated on many stickers (possibly in different words), or because they are supported by general principles.

Most notable is the massive support for the weekly exercise sheets which are peer-assessed and discussed in class during the first hour of the following session. It is also worth noting that there is room for some improvement to this system. I have subsequently spent more time on the wording of the exercises.

The request for structure in the peer review activity is hard to answer. It was my plan to try a number of different approaches and monitor the exercise, but much of the time

I should have spent on this was taken up by latecomers who had missed the previous weeks entirely, or by (the few) students who simply had not done the exercise.

The first weeks following the evaluation I gave them an assessment form, but I was unable to monitor the effect of this. The coming term I will have to look more at what the students actually do, both their answers and their feedback to each other. This should give me the insight to adapt the process to work the way I want.

The demand for sample solutions was answered by publishing a student paper with my own feedback to it. The paper was distinction-quality, but still had considerable room for improvement.

Following the evaluation I have also been more careful to take two breaks during the 3h session. I have also been more careful to make a summary of each lecture. Oddly enough, this appeared both under Continue and under Begin...

Several students commented on the course contents, with 'alter' stickers ranging from «too much theory» to «more technical». It is easy to sympathise with the request for more practical examples and exercises, and I am continuously looking for good examples and exercises to include. However, the module concerns security in complex computer systems, and thus a practical example will tend to be too complex to study without removing significant chunks of the syllabus.

Now, it is a possibility to centre the module around one carefully selected practical problem, more or less according to the principles of problem-based learning (PBL), covering a smaller selection of theory but with a stronger practical link. This could either be as conventional PBL, or with lectures using this problem as a running theme. Finding a suitable problem is not trivial, and the best I can do is to keep my mind open to this approach while I continue to search for practical examples to use in lectures and in learning activities.

It is a problem that the four module conveners responsible for compulsory modules on the programme have never met to discuss the overall course objectives, and how the individual modules fit into the picture. The module coordinator showed no interest in coordinating module objectives either.

I was given the most vague and flexible module title, and was left with the task of shaping this into a module without overlap with the other modules. The obvious solution to this challenge was to steer towards a high-level coverage including general concepts and terminology. One would have hoped that the other modules would provide practical and low-level examples, but with no environment for inter-module coordination, this will only happen by coïncidence.

It seems that the best I can do around these comments is to continue the search for good practical examples and exercises, and weave them into the syllabus.

For me, this exercise was very useful. Most importantly, the support for the weekly exercises was a great confidence booster. It is clear that some of the stickers where outliers or just illegible, but there where more than enough constructively useful stickers.

I probably would have had a very good guess on all the problems and weaknesses myself if I had thought about it, but such an exercise gives more confidence in the analysis. Additionally, the exercise tells the students that I am working on it, and it can be a step towards a more collaborative learning environment. At a subconscious level

(for what that is worth) I feel that it has supported my good rapport with the students.

2.1.6. Project Supervision

My first group of dissertation students, on the MSc, started before I joined, in December 2005. Since then I have supervised final year students (45 credits) from September to March, and MSc students (60 credits) from December to August each year.

Surprisingly, there is very little difference in the level of a BSc and an MSc dissertation. Even though the MSc dissertation is worth 60 credits, it is little more than two months of real work, done in June and July. Until May, taught modules is the priority, and the final deadline is early in August. Thus the British MSc is significantly less advanced than most continental masters degrees which typically have a full year (FTE) of dissertation work.

It is an unfortunate fact that many of my project students have failed their dissertations. I have had to form new hypotheses aiming to explain this every year.

In my first year (Spring 2006), the students started two months before I did, and I was given no information about the degree programmes and the expected background of the students. Assuming that the students studied *computer science* and that this is a mathematical discipline, I proposed projects for which the almost no students were qualified.

Later, it has become evident that this problem of inappropriate topics for the students is widespread in the department. Currently (Spring 2008) the procedures for allocation of dissertation projects and supervisors are under review in the department. It is an acknowledged problem that there is a shortage of suitable topics for Information Systems. Several supervisors exclusively offer topics in their research areas.

During the first years, I had very few of the stronger students. Although poor marks makes the dissertation harder to complete, it was a worse problem that many of my students were not motivated. Motivated students and students with special interests tend to be attracted by supervisors known from taught modules. Since I did not teach in the beginning, I was unknown to the students, and I was given students who did not know what they wanted to do. Some had not even filled in the forms to declare their interests.

Over time I have managed to develop a broader range of topics. I have made software development projects relating to my specialities, so that they require only limited technical understanding. These have gone down well with some students, but are still out of reach for some of the students aiming for a narrow pass.

My role as department webmaster has given rise to some web development projects. Because the university again is changing web system, and therefore has abandoned the existing system used in the faculty before it was complete, this has not worked as well as it should. It seems to work out well enough, but cannot be run again next year.

As described, I have solved some of the problems from the first two years, but still too many of my students do badly. In order to monitor the students, I have scheduled weekly or biweekly meetings with all of them, and I urge them to write short drafts (computer code or paragraphs for the report) for every meeting. This had no effect.

Almost no students meet regularly, and the best I can hope for is to see a few draft pages once during the year.

I have not fully made my mind up about whether this is my problem or the student's. Of course, it will be easy to answer any formal criticism by arguing that if the students had done what I asked them, they probably would have done well. However, it would be better if I could find an approach which inspire the students to work.

It is possible that I harsher feedback would solve some problems. Maybe some students don't need to hear what they should work on, but rather to hear that they need to put *more effort* into it—lest they fail. In some cases this is probably worth a try next year.

2.1.7. Collegial support

Throughout the teaching development, I have often sought advice from colleagues in the department. Particularly, it has been important to check how well my approach fits into normal practice. It is not that I am afraid to deviate, but I would restrict the deviation to cases were it leads to an improvement. Undue deviation serves only to confuse the students, and it takes them longer to figure out my expectations.

Unfortunately, many of the mechanisms which should have been in place to ensure consistency in taught programs are dysfunctional. Programme coordinators have done next to nothing to coordinate the various modules and make sure that they collectively support overall targets rather than compete and overlap.

Over time my ideas seem to be recognised by my colleagues. The MSc programme director wants me as a deputy to coordinate one programme, and I was asked to observe a lecture for one colleague expecting my feedback to be useful. Some of my teaching and assessment methods seem to have caught on well with the one academic who started after me. More senior staff are, in most cases, reluctant to change established modules.

There are no formal fora for teaching support and collegial advice. However, some of my colleagues are very considerate and supportive, and they have been worth returning to for advice. They have given good feedback on the phrasings of assignments, amount of coursework, et cetera.

Much of these support is best provided informally, although it is a pity that appointed mentors for new staff are unable to give it. Some support and coordination should have been organised in formal fora. For instance, it would have been a great advantage to coordinate coursework deadlines. It is quite normal to have bursts of extensions because deadlines pile up and too many students could beat any academic in poor time management.

2.2. Research

My main motivation for going for an academic post when I joined Surrey was to have the stability and freedom to establish a team. A team was deemed necessary to make the most out of my research ideas.

Many challenges must of course be tackled in order to establish an effective team. The most immediate and obvious are the acquisition of funding and recruitment of PhD students and post-docs. Once the people are available, the team must be supervised to run smoothly and effectively.

2.2.1. Grant proposals

In addition to being the first necessary step in establishing a team, research grants are so highly valued by the university that it becomes and obvious goal for all of us.

Proposal writing took most of my time March–October 2007. A total of three proposals were made, a small travel grant to the British Council, a proposal for a PhD student from Leverhulme, and a first grant proposal to EPSRC for an RA for $2\frac{1}{2}$ year. Only the first grant succeeded. Unfortunately, the other two funding bodies did not give any constructive feed-back giving very limited basis for reflection. A second EPSRC proposal was filed in November 2007 and failed.

During the application process, I sought a lot of advice from colleagues in the department. Unfortunately, most of the advice senior colleagues could offer was on the word and punctuation level. Only the Head of Department had the patience to look at the proposal as a whole, and give feedback on structure, objectives, and planning.

Before I came to Surrey, I worked six month on writing and coordinating proposal for other investigators. All those proposals failed, and I am convinced that the main reason is a completely flawed starting point for the process. Most academics want (need) more money to continue their activities as they always have. Most funding bodies award money to create something new. The mismatch is obvious.

Thus, there is a lot I do differently when I can choose the strategy. For instance, understand the priorities of the funding body before starting. In my opinion, the key to a good proposal is a clear concept, including a specific and well-defined goal. Obviously, this goal must fit into the strategy of the funding body, and it must be sold more as a business deal than as an appeal for charity.

It is hard to learn much from my experience so far. The same principles have been applied to all the proposals, and the feedback on the two EPSRC proposals is very similar. The main criticism was on the level of technical detail. I will need to provide more detail in the future.

2.2.2. Change of Research Area

Over the last couple of years, I have gradually changed research area. I wanted a more practical area with clear applications. By making the change gradually, it was possible to maintain a steady publication rate. The change had no clear direction. The original intention was to move into cryptography, but I found more good ideas in digital watermarking.

The motivation for the change was two-fold. Firstly, more practical areas provide more opportunities, both for jobs and for funding. Secondly, I found that in my original, highly theoretical discipline, only a few people would actually have an interest in any

given problem. Thus there were few people to discuss problems with, even at the large conferences of 500 people or more.

Now, I define my area as *applications of coding theory in digital watermarking*. It is an interesting area because the applications are obvious, but very few people have background in both digital watermarking and in coding theory. Thus most of the literature take a too simplified view on one of the two fields.

After I joined Surrey, I have managed to publish my work also in the Watermarking community, in journals and publications with an audience very different from my background. This has been challenging, and I still cannot publish as easily in watermarking as I used to do in coding theory.

The main problem is very different culture and methodology in mathematics and engineering. The logical arguments of mathematics are not always accepted in engineering, instead experiments or rather tests are expected. In a practical field, it is also much more important to put the work into context.

2.2.3. Team management

I had my first PhD student starting mid-June 2007 (officially 1 July), and my first post-doc started 24 September 2007. Unfortunately, I did not manage to find closely related topics for the student and the post-doc. Thus there is not as much room for team work as I would have wanted.

Weekly research meeting

In order to create a forum for collaboration, I initiated and now organise a weekly workshop in digital watermarking. The main motivation for this was to support my own team, but a critical mass is necessary, so it is organised for entire watermarking group. It has been a great success, and the ten full-time members of the group (including two other academics) attend regularly.

The purpose of the colloquium is to be a forum for transfer of knowledge between different researchers, and to be a creche for new ideas. Previous activities in the group had been centred around MSc students, and thus did not allow us to go into the full depth of potential research problems.

Most of the colloquia have been either a prepared talk by one of the members, or discussion of a paper from the literature. Almost all the members have contributed topics. This works well, it is not too difficult to find papers to fill the programme, and prepared talks can be fitted in when people volunteer, usually as a rehearsal before a conference.

It is especially pleasing to observe that the research assistants take active part. They have specialist knowledge on specific fields, and can therefore provide insight which none of the academics have. This has been valuable both on problems raised by the PhD students and on problems raised by me as organiser.

Supervision

So far, I have managed to get the collaboration working the way I want with the RA, but not with the PhD student. The RA and I are able to bounce ideas, and we have complementary backgrounds which makes the collaboration very fruitful and very creative.

Of course, this kind of collaboration requires a mature and well-trained RA, and this is one reason it does not work as well with the PhD student. As with the MSc, I have to get used to the British PhD programme. Most importantly, post-graduate training is not required to start a PhD in England, contrary to any other country I know of.

I have a challenge in bringing the PhD student from a level of mechanical 'lab work' to a level of creative thinking. At the time of writing, he has collected very interesting data, but they are, it seems, for him just data. In order to make a publication or dissertation the data must be interpreted, and the interpretation sold as a valuable contribution.

In the system I am used to, the required level of creative thinking and interpretation is reached prior to starting a PhD, but I do understand that it is quite normal that it is not in England. It is not obvious how to solve this challenge completely, but two upcoming processes are expected to help.

Firstly, the half-yearly progress report for the PhD student is overdue (delayed due to a paper deadline and holidays), and will have to be completed in April. A meeting with the secondary supervisor is normally part of this process, and thus it provides an opportunity to discuss my concerns with both the students and the secondary supervisor in a formal context.

The second project, due to start 1 October, is to supervise a student jointly with Dr. Nick Antonopoulos. We have the topic and the funding, and a very qualified student has accepted. Dr. Antonopoulos consistently graduates students on time, with a number of publications. Furthermore, the two of us communicate well. Hopefully, running a joint team will let me understand how he does it, and I will aim to extend good practice to the rest of my team.

2.3. Administration

Administration overlaps with the other two areas. Under this header I will only cover administrative tasks which do not fit into either of the other headers. I think that my most valuable administrative contribution is the research meetings covered under 'Research'.

2.3.1. Web Master

My main administrative duty has been as department webmaster. I have been able to make some good improvements to the web pages, in spite of the (lack of) support available from the faculty and the university.

The servers and systems for web pages have changed approximately once per year over about five years, leaving a host of legacy systems still in existence. When I took over,

the pages had just moved out from portal, into a local template using DreamWeaver. No proper training with DreamWeaver was provided, and it is doubtful that the software is suitable for a site of our size even with proper training. I encountered several problems which I was unable to solve.

In Winter 2007, a new faculty-wide content-management system was introduced. This had been developed in-house based on a PhD-student's work; the student himself no longer available. When it was launched, it was still full of bugs, and several promised features were missing. It was partially patched during the Winter, but because of the university restructuring, insufficient resources were available.

We did eventually manage to move into the new system in April/May. In June we had to redo several pages, because the new rebranded layout was incompatible with the old one.

The web pages remain largely out of date, because it is almost impossible to get up-to-date information from other staff. Responsibilities are unclear, and in most cases neither the programme director nor the programme administrator know who has the most recent information.

Some achievements have been made over the years. We have revised the admissions pages and the research pages. The main priority has been to establish a visual façade, as well as updating some of the most important information. Those who have commented on the changes have recognised it as significant improvements.

2.3.2. Time management

There is no doubt that the academic workload is high, and that our department is understaffed. This means that not all tasks can be undertaken to perfection, and it is necessary to prioritise.

A more interesting challenge than the size of the workload is its diversity. It is necessary, at any point in time, to keep track of a large number of important tasks and their deadlines.

Their is a significant danger of becoming like a *Den Stundesløse* [Hol31]. An over-busy business man who never is able to complete a task before he starts panicking about another. Although not as extreme as the comedy character, I see some such symptoms in some of my colleagues, and I sometimes have, consciously to drop important tasks to get any work done at all.

Good time management under such conditions is a key skill, which is still under development.

2.3.3. Other activities

Erasmus

Summer 2007, I took over as academic contact for Erasmus student exchange in the department. The department had no tradition for Erasmus exchange; nobody knows of

a student ever going out, and the few incoming students have come on programmes in Electronic Engineering.

I took it on as my task to raise the awareness of the Erasmus programme, among staff as well as students. It appears to me that very few students know about the opportunities, and hence it is impossible to say if the low participation is due to ignorance or lack of interest.

It is too early to observe any results. So far I have made a web page and urged our UCAS speaker to adopt two slides of mine. There is no case for raising the profile of Erasmus beyond that of our Professional Training Year, so a massive PR campaign is out of the question.

Collaboration

One of my probation targets is 'to become involved in the wider research programme with other researchers' in the department'. Unfortunately, more senior staff do not have similar targets, and it does take two to collaborate.

The weekly research workshop is some progress towards this target, but otherwise there is very little to be involved in. Some opportunities have been investigated, but it has been impossible to muster the necessary joint commitment to get any results.

Nothing is better for research than good collaborative links and fora for discussion. However, collaboration for the sake of collaboration is a time waster when one does not quickly hit it off together.

I find it a good strategy to be open for collaboration, but also to drop ideas quickly if mutual commitment is evidenced.

2.4. Conclusion

In this chapter I have focused on what I have spent time learning, and what I am still working on. A conclusion would be premature—even though a lot has been learnt, I am still on my way forward.

3. Project: Revision of a taught module

The first module I was given to teach at Surrey, was a new module on *Steganography*, titled *Secure Information Hiding* (CSM25). There is a number of reasons for why this became a particularly challenging task. After the first run of the module in Spring 2007, it became clear that a complete revision is necessary.

3.1. Background and context of the module

CSM25 was to be designed as a core module for a new MSc programme in *Security Technologies and Applications* (STA), to be taught for the first time 2007/08. The module, however, would start in Spring 2007 as an optional module for other MSc programmes in *Internet Computing* (IC) and *Information Systems* (IS). The module description can be seen in Appendix F.

The two traditional MSc programmes attract very different audiences. IS originates from an old conversion degree, and mainly attracts students with little or no background in computer science or computer programmes. IC, on the other hand, requires a sound knowledge of computer programming. It was generally known that teaching for both programmes is extremely challenging, and few modules are indeed shared. STA would aim for an audience similar to IC, and later experience indicate that this has been achieved.

Steganography, the topic of the module, concerns secret communications. Contrary to traditional cryptography, steganography requires the very *existence* of secret communication to be secret. Contemporary solutions mainly aim to hide the secret information in images or other media files, using imperceptible changes to the medium. It thus forms part of information hiding, together with watermarking which hides non-secret information in multimedia files.

Steganalysis solves the problem of the adversary. It aims to detect the presence of steganography.

In the context of STA, the module has an unusually narrow scope, squeezed between separate modules on Watermarking and on Cryptography, as well as *Introduction to Multimedia Security* which is a prerequisite for the three others. Steganography is still emerging technology, and new solutions are proved insecure relatively quickly.

Several textbooks were suggested early in the design process, but none of them contained the technical detail expected in a degree in engineering or a mathematical discip-

line. A reputable, and suitable, book on Watermarking is rumoured to include Steganography in the next edition, but this has yet to appear in print.

3.2. Module design 2006/07

3.2.1. Objective

- Everybody should (in order to pass)
  - Implement a few stego-systems
  - Implement a few methods of steganalysis
  - Learn general principles for secure communications
- To do well, we also expect you to
  - Be able to assess security and reason around different approaches
  - Have an overview of steganography including cryptographic approaches as well as data hiding
  - Understand the theoretical foundation for techniques implemented.

To summarise this in general terms, the pass mark requires both a basic procedural skill and some declarative knowledge. To do well, some functional understanding – ability to assess solutions – was required. Some ability to *relate* the material to basic theoretical subjects studied previously was expected.

3.2.2. Contents

Steganography has been studied by two distinct research communities, namely in Cryptology and in Signal/Image Processing. The two communities use non-equivalent definitions of Steganography, and they use different methodologies. I wanted my module to cover both approaches. A focus on the contrast between the approaches would be the concept which gives CSM25 a distinct identity among the other STA modules.

When the planning of the module started on the assumption that a textbook could be used as a basis. Senior staff suggested a handful of possible books. However, none of these books proved adequate. Most of them were old, shallow, and non-technical. It is possible that they could be used as textbooks in a non-technical module, but that is not a kind of module I would be qualified to teach (at that time).

There was one book that I found useful, not as a core textbook but as a very good supplement. Like the other it did not offer the technical detail to enable the students to implement solutions. However, it raised many interesting philosophical and ethical issues; like who need the technology and why.

In general, I found less literature than I had expected, and composing a good syllabus proved difficult.

The most significant chunk of the module became implementation of basic techniques for image steganography and steganalysis. This could relatively easily be facilitated by selected articles and precise lab exercises. These methods represent the secret message by imperceptible modifications to an externally given image (known as the cover image).

Because many students lacked the background in programming and implementation that is normally expected computing, the syllabus was extended to teach the students good programming practice as well. Basically I wanted them to write good programs which are easy to reuse—essential if different exercises are going to build on each other.

One or two weeks were spent on steganography by cover synthesis, i.e. no cover image is externally given. Instead an image or text is synthetically generated by the algorithm to represent the secret message while looking innocent. These algorithms were clearly too complex to be implemented and tested by the students.

One cryptological paper on steganography was used. This introduced a strict security model. The problem is that this model arguably is too strict; so that cryptography, for the time being, is unable to provide practical solutions.

The final topic, the first as it happens, was on *Kerckhoffs' principles*, introduced by Auguste Kerckhoffs in 1889. The essence of these principles are regarded as imperative in modern cryptography, and have been instrumental in establishing the mature and highly trusted cryptographic technology in use today.

The image steganography community has largely ignored Kerckhoffs' principles. Thus this topic has a potential for engaging the students in intelligent discussion and reasoning. Should the principles have been as imperative in steganography as in cryptography? Why/Why not?

3.2.3. Teaching and learning activities

Every MSc student in the department were given a laptop at the start of the year. This is a controversial scheme, and after the trial in 2006/07 and 2007/08, it was abandoned. It was never clear whether we have it as a teaching tool or a marketing tool. In the end, it probably proved too expensive as a marketing tool, and under-utilised (by the lecturers) as a teaching tool. In any case, at the time it allowed me to combine lab exercise and lectures in a joint session in a regular teaching room.

I decided to take full advantage of the laptop scheme, to interleave practical computer exercises in the lecture; primarily encouraging the students to test features and techniques immediately as they were explained. I had been advised against setting exercises intended as homework, as few students bother to do them.

On two occasions, I used discussion exercises to work through more philosophical aspects of the syllabus. In both cases I used first large groups and subsequently a plenary discussion. The first exercise was simple and worked well. They had to list and prioritise a set of design principles.

The second exercise had a couple of interesting flaws. The class was split into two group (pseudo-randomly). I had phrased a statement which one group should defend and the other argue against. The class nominated a student to chair the discussion. The

intention of such an exercise is to engage the class fully in the issue in question, and avoid the limitations of teacher intervention.

Problem no. 1 is that the chair tends to be one who wants to be very active in the discussion. This probably should have been anticipated, but it is also very hard for the teacher to chair the discussion without steering it.

The second problem was that the discussion headed off in the wrong direction because the basic terminology was not clear enough. Obviously, it was a useful exercise in that this problem was identified. However, it would have been better to have a less formalised discussion with an active teacher at this stage of learning.

3.2.4. Assessments

The assessment was based 40% on a unseen, written exam, and two relatively large coursework assignments of 25% and 35%.

The coursework was essentially programming, including testing and evaluation, but with very little opportunity to demonstrate analytic skills or relational understanding. On one hand, this programming is an essential learning activity. On the other hand, it is a bit limited for assessment.

The exam was skewed towards terminology with many questions for definitions. These questions made it feasible to make the well-defined, detailed marking scheme expected in the department. Without a core textbook, I found it unfair to ask questions not thoroughly covered in lecture.

3.3. Experience 2007

3.3.1. Student evaluation

At the end of the term, I asked the students to fill in an evaluation questionnaire. Ten out of 13 students responded. The questions and answers are shown in Appendix B.

As can be seen, a clear majority (7/10) was satisfied or very pleased, and an even clearer majority learnt much from the module. Not surprisingly, the high learning and high workload replies match in numbers.

Thus, the student feed-back does not give any great reason for concern in itself, but the workload should be reduced in a revision.

The feedback on specific teaching methods and learning activities is interesting. Nothing stands out as particularly bad. Each activity is deemed to be satisfactory to at least half of the students.

It is surprising that half of the students gave the web pages the highest score, as they were only intended as a kind of secondary support. The praise is welcomed, and the web pages need to be continued.

The coursework was satisfactory to the largest proportion of students (8/10), supporting my view that learning by doing is the key to good results. It is just unfortunate that the coursework covers too narrow a selection of the syllabus.

There was a strong positive correlation between the student opinions of different learning activities. In other words, students who were dissatisfied with one means of learning tended to be dissatisfied with all of them.

The students feedback tends to encourage the integration of exercises and lab exercises, although not by a clear margin. Additional comments tended to request more examples in the lecture.

3.3.2. Student assessment

Coursework

Overall the students did well in the coursework. They generally acquired the skills I asked for, both in terms of steganography algorithms and in terms of good programming practice.

Some students only learnt enough good programming practice by the second piece of coursework, and for those students it was unfortunate that both counted in the mark. More supervised exercise work prior to the first assessment would be fairer.

Exam

The exam showed that the learning outcomes were largely limited to image steganography and steganalysis. In other words, material related to the coursework had been learnt, and other material had largely been ignored.

It was particularly depressing that many students had totally missed all the cryptological material covered. This problem can be explained by a lack of alignment between the exercises/coursework and the syllabus (assessment). The coursework covered only a narrow selection of the syllabus, and most students have probably not done the other exercises.

3.4. Revision 2007/08

After the first run, it was decided to remove CSM25 from IS, thus allowing me to assume proper programming skills as a prerequisite.

3.4.1. Revised Objectives

The revised objectives were presented to the students as follows:

- Pass (50-60)
  - be able to implement simple stego-systems and steganalysis techniques
  - have an overview of the different techniques for and approaches to steganography
  - use the basic terminology correctly and unambiguously

- Distinction (70+)
  - Be able to generalise theories and techniques in steganography, and relate and contrast different approaches.
  - Be able to assess security properties in a communications system, and assess security needs in an application.
  - Be able to discuss stego-systems in unambiguous terms, and choose appropriate approaches for given application needs.

Again, the pass mark requires both basic procedural skills (programming) and multi-structural knowledge.

The old basic objectives focused too much on implementation, given that implementation was not feasible in the cryptographic topics. This motivated the new objective on basic terminology, and much of the breadth is evidenced in conflicting definitions. The 'general principles for secure communications' was removed because these principles were not sufficiently well supported throughout the syllabus.

In the advanced criteria, the objective of understanding theoretical foundations proved to be infeasible. Only students with strong theoretical first degrees could be expected to achieve this. The new advanced objectives are fairly general and standard – they could probably have been phrased without knowledge of the field. If the new weekly exercises, and the concluding essay for the portfolio in particular, have worked as intended they will have prompted reflection over questions relevant to these objectives.

The distinction requirement should probably be read as 'two out of three', with one out of three being a merit, and three out of three being 80% or better. The merit band was intentionally left out to indicate the room for interpolation. It would probably have been better to label the advanced criteria as 'perfection' rather than 'distinction', to reflect the fact that distinction is a wider band than perfection.

3.4.2. New assessment pattern

Because the assessment pattern has to be defined in the module description in May the preceding year, the new pattern had to be chosen based on only a preliminary review of the module.

Two issues stood out as obvious.

1. The practical (non-compulsory) exercises were not effective, and assessment proved that topics not subject to compulsory coursework were generally not learnt in the same depth. A scheme encouraging students to do exercises continuously should be sought.

2. Making a good and fair, unseen examination on a course without a proper textbook is very difficult. The main problem is that there is no well-defined body of knowledge which everybody is supposed to have read. Therefore, all assessment in this kind of module should be coursework-type.

Admittedly, it is not obvious that the first issue has to be solved through assessments. However, assessments do provide a potential solution, and therefore we address it here. The value of *active learning* is also well-documented in the literature. Most people learn and remember more from what they *do*, than they do from *watching* or *listening* [Big03].

Assessment based entirely on coursework is controversial, and the Board of Studies is generally worried about plagiarism, collaboration, and hired services. As discussed in the sequel, I have taken some measures to limit such problems. The greatest advantage of coursework, as I see it, is that it directs the learning process, and it ensures alignment in that the students are assessed in what they were explicitly asked to learn. This can be achieved in unseen exams, but it is harder.

It would be beyond the scope of this report to dig into all the possible advantages and disadvantages of coursework-based systems in general. The main rationale was that a fair exam was infeasible.

It should be noted that making a written exam is not impossible, merely difficult, and this is partly due to local practice. A written exam is expected, in the department, to have very precise questions with fine-grained marking criteria. Now, the literature does give examples of more flexible questions in written exams. The main advantage of abandoning the written exam is that the procedure is less formal, and the examiner is given more leeway. Hence coursework makes it easier for me as a lecturer to experiment with different types of problems and deviate from standard practice in the department.

Two assessment exercises were suggested by Andrew Comrie [Com07].

- Weekly exercise sheets with peer-assessment every week. A (possibly random) subset is specified and required for end-of-term assessment.
- Group projects where the output is presented to class using a poster.

The first item appears to be of critical value, as it creates an incentive to do exercises every week. It combines learning and assessment in one exercise, and thereby it ensures alignment of the module.

Whereas the weekly exercises ensures breadth, the poster session was adopted to encourage depth on a subtopic chosen by the students themselves. It is hoped that the posters will be quick to assess. With a class of about 30 student in 10 groups, two three-hour poster sessions are planned. The assessment should be completed within the two sessions.

Portfolio

The contents and assessment criteria are shown in Tables 1 and 2 respectively. It is admitted that the end points in the criteria are intentionally left vague. In the failing end, it was deemed useful to get criteria for compensation band papers, i.e. that they have sound declarative knowledge on some (more than one) relevant topic, but still being short of a pass. The 0-40 band is a large one, but it is doubtful that it is worth the time to clarify any ranking of different non-compensatable failures.

Table 1 Contents of the Portfolio

The portfolio should be composed of the following items. The portfolio should be written as a coherent document, so that the different items support the conclusion made in the final essay, and so that it collectively display that you have covered the full range of the module contents.

- Two of the weekly exercise papers to be specified (by me) in Week 11.
- 1-2 items of your choice. These could be additional weekly papers, or other pieces of work of similar extent (essays or exercises). The items should be chosen such that the portfolio demonstrate a good breadth of understanding, and support any conclusions in the last essay (see below).
- A concluding essay (1 page, maybe 2), summarising the highlights of what you have learnt in the module. You should address some of the following points
  - Why are the chosen highlights particularly important/interesting for you?
  - How do these highlights relate to other topics you have studied?
  - How do the highlights relate to real-world applications (such as your future career)?
  - How have the other items in the portfolio helped you to learn (or show that you have learnt) these highlights?

Table 2 Assessment criteria for the Portfolio, CSM25 Spring 2008.

less than 40	Clearly failed to reach the learning objectives.
40-50	Sufficient declarative understanding is demonstrated in some of the items, but the student has failed to cover a sufficient range of the lectured material.
50-60	The portfolio shows a declarative and procedural understanding of the material lectured.
60-70	Declarative and procedural understanding as above. Sound structure with clear focus and (almost) no irrelevant material. Some attempt has been made to see the covered material in context, but not quite at the level of a distinction.
70-80	Structure and understanding as above. Sound evaluations with good arguments. Connections are drawn between the different problems included, and the material is put into context. Opinions are backed by sound arguments.
80-90	Structure, understanding, and argumentation as above. The student is clearly aware of his own learning from the module, and can see this in relation to real-world challenges, other modules studied, and/or future career plans.
90-100	Beyond any expectation.

At the high end, it seems to be common practice that a perfect paper is given a mark in the 80-s (at best). The 90+ band is reserved for the truly outstanding and unexpected performance. My wording reflects that — beyond expectation is a performance I cannot predict. If I had been able to describe it, I would also have been able to expect it.

The wide bands at the end appears to me as a very English construct. The Chinese also use percentages, but in their system any normally sound performance should be in the 90-s, giving a much narrower distinction band. In countries using letter marks, an 'A' is likely to compare to distinction, and no subdivision is possible.

It may be argued that the assessment criteria do not match the learning outcomes. This largely because I managed to find better words by the time the portfolio was assigned.

The best example is probably the 80–90 band, where I ask them to relate the material learnt to real-world applications. In my mind, such ability correlates well with the ability to assess security properties (in real systems), relating and contrasting different approaches, and assess security needs in applications. The link is admittedly not a strong one.

I do not find the learning outcomes concrete enough to prompt optimal thought processes in the students. I am not convinced they have to be, as the students will be prompted by smaller assignments rather than the description of the module as a whole, but the learning outcomes will surely be revise again.

The portfolio assessment criteria were to a greater extent designed to prompt appro-

priate thought processes. It seems reasonable to expect that a large number of strong students in the class be able to relate the material learnt to real-world applications, and that this will enhance their overview of the field and high-light relational understanding. Even though the match with the learning outcomes is suboptimal, I expect relevant understanding and ability to be demonstrated.

The contents, as described in Table 1, comprise five elements. The concluding essay has a largely different purpose from the other (3-)4 elements. The weekly exercises, leading to the 3-4 main elements, are designed to demonstrate basic knowledge across the breadth of the syllabus. In most cases, the exercises are too small and to the point to allow a proper demonstration of relational understanding. The essay is intended to add that room for reflection and relational understanding.

For this reason the portfolio can only be assessed as a whole. The main items will be essential in distinguishing between passes and failures, whereas the essay is absolutely essential to award distinctions.

The weekly exercises underlying the portfolio is the basis for the module design. One (two in a few cases) key points have been made the topic for the weekly exercises, and the exercise defined the learning expectation. The lectures were intended primarily to enable the students to do the exercises, secondarily to fill in a bit of context.

It is a worry that the weekly exercises may not sufficiently have prepared the students for an assessment of relational understanding. As far as the assignment and written paper goes this is probably true. Hopefully peer assessment and class discussion relating to the weekly exercises have given the necessary grounding to develop relational knowledge. It will be interesting to see what level of understanding the assessment will show.

Poster

The poster project has many traits in common with activities used in other modules in the department. At least two modules ask the students, in groups, to present a chosen paper to the class. In one case this material is not assessed at all. In the other case there is a viva voce examination, where the students are expected to know the paper they presented themselves, but not papers presented by others.

Since the presentation is the primary opportunity for depth study in the module, it is, in my opinion, the best opportunity to assess deep learning and relational understanding. The topics actually chosen are listed in Appendix H.

There are issues with both of the assessment exercises. Working and largely collaborating on the weekly exercises over the course of the term, students are likely to make very similar answers. Especially for programming exercises, the answers should be expected to converge. Comments in the programs becomes a means to display individual understanding. Also commentaries and self-evaluation are used where possible.

Group work is always controversial due to the risk of free-riders. We will therefore make half of the mark individual, by assessing each students contribution during the presentation of the poster. Admittedly, it is hardly possible to make a complete assessment within the short time of the presentation. The principal aim is to penalise free-riders who either have not made a sufficient contribution to the team effort, or have

insufficient appreciation of the team output as a whole. If this can be achieved, this part of the mark serves its purpose.

Another issue with the poster session is capacity. Present numbers, of about 30 students, is the limit for the present form. In a larger module, it would be impossible to present all posters to the entire class, and the presentations might turn into dedicated assessment sessions. If this were to happen, one could argue that the presentation should be made longer to enable a more accurate individual assessment and marking. On the other hand, viva examinations are very time consuming for large classes, and it is unlikely that we would be able to justify the resources. As a minimum, one would have to consider assessment based on a single submission (portfolio) for each student.

Other lecturers running paper presentations in their modules confirm that they consider it unscalable for larger classes. There is also general criticism against the department as a whole that we over-assess, and that we do not have the resources to continue to spend as much time on assessment.

The Weekly Exercises

The weekly exercises has become a core for both CSM25 and CSM27. The exercises are designed to cover the essential material of the module. In fact, the exercises are, in most cases, designed first, and the lecture is developed to get the students started. Assuming that exercises are necessary to develop sufficient understanding, this is ideal.

Exercises are assigned every week. The first hour of the subsequent session is used to discuss the exercises. This hour is flexible. The ideal is peer assessment, where the students discuss their solutions in pairs or small groups. With the lecturer present, any arising questions or difficulties can be dealt with immediately. This does not always work, however.

Students who have not tried to do the exercises before the session can work on it in class. However, sometimes most of the class has failed to solve the exercises, even when trying. In these cases, a plenary discussion is necessary. Usually, there are enough ideas in the class to make it a discussion more than a lecture.

There are various variants of the system. The basic idea [Com07] was, at the end of term, to draw a random subset of exercises and require the students to hand in this subset. A more extreme variant [Big03] is to require the students to hand in all the exercises, but only two mark a random subset. Biggs reports an instance where this was tried, and the result was that the students handed in much better papers than they did when all the papers were to be marked.

I stretched the system to allow the students free choice for two out of five items. Furthermore, I extended it more to a portfolio by requiring a concluding essay as one of the five items. The last two items are nominated by the module convener shortly before the final deadline.

In the concluding essay, the students are asked to put the taught material into a wider context. This can for instance imply real-world applications or relations to other taught modules. The intention of the essay is to enhance the opportunity to demonstrate deeper learning, and it is anticipated that it will be instrumental in distinguishing between

straight passes and merits or distinctions.

The deadline for the portfolio is set such that the students have time to revise the material, but probably not time to do exercises from scratch. Initially a week was suggested, but this was extended when the deadline had to be set in a very busy period with other deadlines and exams.

3.4.3. Experience Spring 2008

As the Spring term is not yet concluded, a complete evaluation is not yet possible. Still some experience can be analysed even at this stage.

Weekly exercises and student workload

The weekly exercises have not worked as well as they should. Many students are several weeks behind schedule. There are at least three reasonable hypotheses

- The students do not spend enough time on the exercises.
- There is too much work.
- They need more support and supervision on the exercises.

The last hypothesis is almost certainly true. Many students struggle to make their ideas work on the computer. When this came to my attention in week 7, session 8 was postponed to give room for a lab session instead. This brought many students a big step forward, and many questions were answered. Next time the module runs, supervised lab time has to be scheduled, possibly by spending less time on peer assessment.

The second hypothesis, about the workload, is probably true as well. In hind-sight the workload does not seem to have been reduced compared to last year, it is just distributed in a different way. They save the revision for the unseen exam, but have the poster project instead. Instead of preparing two large pieces of coursework, they are supposed to do smaller pieces every week.

The first hypothesis, blaming the students, leads to another controversial question. What is a student working week? For most purposes, a working week is close to 40 hours. In practice, it is of course optimistic to believe that most students spend this much time, but should such beliefs influence on expectation?

In most countries, where higher education is not run as commercial businesses, one would usually stick with the conservative expectations. If students choose to spend less time, it is fair to expect them to fail. However, the established attitude in this country, as suggested by senior staff in the department, is that the syllabus has to be adjusted to fit the time the students are willing to spend, estimated about 20 hours per week. (And probably declining.)

Comparing CSM25 with CSM27 in the Autumn, lack of student effort seems to explain very little. In CSM27 most of the students managed most of the exercises, and the same students seem to struggle in CSM25.

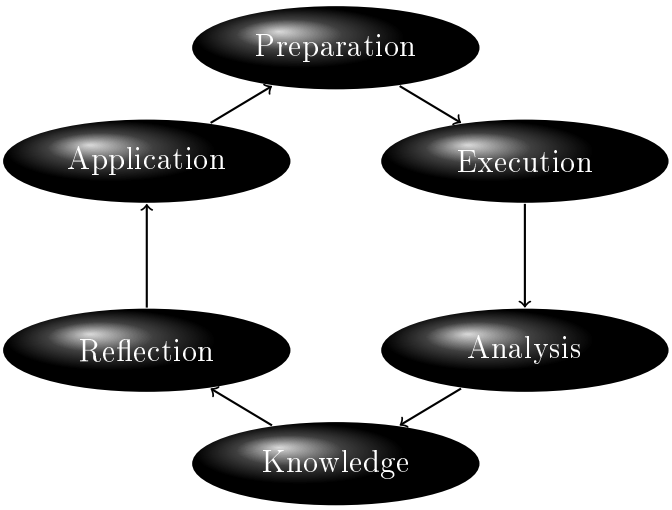


Figure 3.1.: Cycle of experience after [nsf97]. Translations by the author.

Teacher workload

The poster project was introduced as an efficient way to assess deep learning. The assessment in itself still seems to be a quick and efficient task, but the project as a whole is not. Finding good projects was a challenge. Making sure that the students understand the exercise, and discussing the topics with them to ensure that they have a viable approach were quite time-consuming tasks. Finally, some groups (the most promising ones) have enquiries which deserve proper answers.

Overall the current assessment scheme is not sustainable if the class size increases, and the department has ambitions and expectations that it will. Furthermore, the department is starting to deliver modules in China (Dalian), where even larger classes are expected.

Experience Cycles

The experience cycle (my translation) is a learning model I have used before [nsf97], and which explains some of the issues considered in the design of exercises. It is very similar to the Lewinian Experiential Learning Model [Kol84], which has later become known as the *Kolb Learning Cycle* or Kolb's Cycle of Reflection in the English language literature. The cycle models both student learning and teacher activity.

The cycle is depicted in Figure 3.1, and the process can start at any step of the cycle. Typically it may start with a task which is first *prepared* and then *executed*. To give any significant learning these steps must be *analysed* so that they lead to *knowledge*. If we want to learn at a functional level, *reflection* is needed to make the knowledge active so that it is *applied* in the next round of the cycle.

We are aware that some terms and steps may be overlapping, but the principle is useful. In a taught module, students do exercises, and hopefully they go through the

cycle so that they acquire *functional knowledge*. Teacher interaction is available at several steps. One would hope that it is available at all stages, but that's normally not the case in a conventional university model.

The teacher starts out with very limited knowledge when the first exercises are prepared. Only by analysing the students' effort and results, can this knowledge be enhanced and applied in the design of subsequent exercises.

Based on this model, there are two points worth noting. The first point is made in the PGCAP literature, e.g. [Big03], namely the importance of reflection. The students must be prompted so that reflection is catalysed, and teachers must use feedback and reflect in order to improve the next round of preparation.

The other point, which I have not seen explicitly in the literature, is that rapid cycles may give more individualised teaching and support. A typical university module manages one cycle per delivery. Assessment and evaluation is done at the end of the module, and analysis and reflection have to be done between terms. Thus any understanding gained will only affect the next cohort, who do not necessarily have the same background and attitude.

Another problem in the traditional model is that the students receive no feedback and support during the reflective phase. In other words, only a small fraction of the learning process is actually supervised and supported.

The weekly exercises are there to provide rapid cycles. Peer assessment has, at its best, made some students analyse and reflect on their performance. It is important that the exercises include questions which prompt analysis and reflection. However, at other occasions, the students got stuck in the middle of the planning or execution phases, thus never getting to analysis. Furthermore, I did not manage to get information about the student performance every week, so the teaching did was not subject to rapid experience.

Organised lab sessions should in the future help getting the students through the first stages, and through to analysis and reflection. A complete review of student papers every week is not feasible, but some time could be invested in reviewing a few selected papers.

It could be an approach to reduce the number of 'execution' exercises, and have dedicated analysis and reflection exercises. This could potentially deepen the learning on the topics covered, but would require a reduction of the syllabus.

In the next iteration of my own experience cycle, the focus should be on better support in organised lab sessions, and acquiring more information on student performance. Too many changes at the same time muddles the pictures and would make it impossible to analyse the effect of each change.

Contents

Only minor changes were made in the syllabus. Most importantly, I wanted to include some more advanced topics, especially in steganalysis. Some some topics were narrowed down; variants were ignored while the core idea was enforced by an exercise. One topic was completely removed, namely steganography in GIF images. It was felt that the learning on this topic is primarily on image representation, and only marginally on

steganography. Good students would find it easy to read up on this topic on their own.

Suggested improvements

First priority for next year will be to ensure more organised lab time with teacher support. It is hard to say if this is sufficient to get the students through the exercises, or if the syllabus should be trimmed down somewhat as well. It is possible that the time taken by supervised labs will force a reduction in the syllabus.

I will consider abandoning the poster project, to save time, both for the students and for the teacher. This would increase the weighting on the portfolio which would then require some extra quality assurance. It might be reasonable to require a complete set of weekly exercises in the portfolio. This decision will not be made until we see the results both from module evaluation and from student assessment.

3.5. Conclusion

The weekly exercises have led to a better rapport with the students, but is not yet sufficient. Most importantly supported lab time is necessary.

The new assessment scheme appears to be fairer due to better alignment. Only topics where they have been asked to do exercises are assessed in the end.

The workload has to be considered again, and possibly reduced. In short, we have improved the module, but further improvements are necessary.

4. Conclusion

An accurate self-assessment in PGCAP is almost impossible. The course contents is too fragmented, and different lecturers clearly have different views on the objectives and assessment criteria. As requested, I will here go through the PGCAP learning outcomes as given in [pgc07, p. 8], and comment on my achievements towards them. I will summarise my experience with the portfolio as a learning and assessment tool, and finally summarise my overall PGCAP experience.

4.1. On the PGCAP learning outcomes

The focus in this portfolio has been on how I improved my teaching by experimented with and integrating new ideas and models from different sources. I think I have done well on this aspect, by finding an approach which works for me, and which is supported by a range of sources. This, I think proves the following learning outcomes from [pgc07]:

- (A1) ... understanding of the conceptual models, theories and frameworks underpinning academic practice and their application to complex and specialised contexts
- (B2) ... synthesise new principles and understanding of approaches to academic practice for the improvement of practice
- (C1) ... apply a conceptual understanding of learning and teaching to the planning, delivery and evaluation of effective teaching sessions and/or a curriculum.

It is admitted that my understanding of 'academic practice' is more pragmatic than academic. At a theoretical level, I am familiar with very basic models and principles, but I am able to apply them widely and use them to develop effective methods in my academic practice. This, I take it, is most appropriate for my role, but the learning outcomes could be read to expect wider academic knowledge.

The portfolio has sought to document the evolution of my understanding and application of the ideas above, and thus I think it also supports the learning outcomes of

- (C4) ... identify and reflect upon emerging changes in their own practice for the purposes of continuing professional development.
- (D4) ... engage in self-evaluation and critical reflection for the improvement of practice.

- (C2) ... use a range of sources of evaluative feedback to enhance reflective practice ...

- (B1) ... analyse and evaluate the effectiveness of alternative approaches to academic practice.

Given my understanding is more pragmatic than academic, the analysis in B1 has not been advanced. It has been largely based on very basic, well-known, and almost obvious facts. However, I do evaluate the approaches I try, and I have found that even the very basic facts lead me to effective approaches.

Research abilities have, for good reasons, been less important in the portfolio work. As I have mentioned, B4 (below) was largely achieved before I started at Surrey, and my experiences so far with the First Grant indicates that C3 (below) has been achieved as well as it reasonably can within the time frame.

- (B4) ... demonstrate self-direction and autonomy ...

- (C3) ... effectively plan, resource, implement and report research activities

Obviously, B1 (above) should also be achieved in research, in addition to teaching as addressed above. In the case of writing grant proposals, I do contrast my own approach with observed approaches. A major limiting factor here is the length of the learning cycle. A grant proposal easily takes six months to prepare and another six months for a decision. Hence takes a long time from the work is planned until the experience can be analysed. The cycle for publication is usually longer, typically with 1-2 years from submission to acceptance.

Research has not been covered in great detail by the PGCAP course. It is hard to see how we were supposed to achieve the outcome of

- (A4) ... understanding of strategies for developing [...] research profile ...

The two sessions on publication and grant proposals were basic and did not go significantly beyond the obvious. I have reported that I have had a strategy for several years, including a change of field, and that this, over time, has lead to results. It is not a great academic understanding, but it has produced results.

Hopefully, this report appears, also to the reader, as a confident communications on my ideas and practice, thus meeting the expected outcome of

- (A1) ... confidently communicate [...] about the principles and practice of professional activity ...

Orally, I think this has been achieved in my discussion with and quests for feedback from colleagues in the department. Thus I think I have also achieved the following,

- (A2) ... understanding of the importance of articulating and justifying personal approaches ...

as good articulation and justification have been necessary to obtain the most constructive and useful feedback.

The achievements on collaboration and teamwork are limited, thus the following was only partly achieved,

- (A3) ... work collegially [...] through team work, negotiation and leadership.

I think I have done very well with leadership and teamwork in my First Grant (as reported), and I am developing the collaboration with my PhD student. However, between academics, the university is not a good environment for collaboration. One problem is that collaboration requires a surplus of time; under present conditions tasks are executed by minimum effort. A second problem is that the university does not seem to value collaborative achievements well enough. Authorship is valued, but managing and developing team to author many papers is not, in itself, valued. In grant proposals, the emphasis is on the PI, and CI-s get marginal recognition at best. It may seem that PGCAP is out of synch with the Academic Practice.

One outcome has not been documented:

- (B3) ... integrate disciplinary research or scholarship in learning and teaching ...

No strong integration has been attempted, but it is quite clear that there are synergies between current teaching and research activities. The development of new modules has emphasised potential research problems, and directly aided the supervision of my PhD student. The dissertation students are sometimes integrated into research, but in most cases their training is not sufficiently technical for my own area.

Two learning outcomes have not been tackled in any significant way,

- (A3) ... understanding the role of quality assurance ...
- (D2) ... competently and independently undertake a research task or enquiry ...

Although quality assurance was covered in PGCAP, it was not backed by exercises nor practical work, and I have had no significant, direct involvement in quality assurance exercises in the department. Quality assurance has a strong tendency to be degraded into formal paperwork, whereas real achievements on quality is a product of reflective discussion and negotiation. The department has no forum for such negotiation.

The PGCAP Handbook overemphasises research into academic practices. Participants from a science/technology background do not have any background or training for research in social sciences, psychology, or education, which would be relevant for a research study of academic practices. Such research methodology is far outside the scope of PGCAP.

Therefore, no such research has been attempted, and this decision was supported by the new course leader. What I have made is a reflective report on a professional process. Hopefully this has proved the ability for further development and sound professional practice.

4.2. On the portfolio

This portfolio has been a useful exercise, in that it has been an excuse and incentive to work systematically with self-review, and thus it has contributed to quality improvements.

However, it has not had the portfolio feel as described by Biggs and which I attempt to incorporate in my own modules. The portfolio requirements and procedures were only made clear once the taught sessions had concluded. Hence the portfolio has not been the learning tool that it could have been throughout the module.

The taught sessions now appear to be a distant past. There has been little opportunity to work through the taught material again under supervision. The portfolio has been the most valuable part of the course, as it has been practical work under supervision.

At least two potential improvements could have added value to the PGCAP portfolio. On has been mentioned, by using it as a learning tool supporting taught sessions. The second is mentor support in the subject area. Unfortunately most appointed mentors in the department are both unfamiliar with PGCAP and incompetent as mentors in general.

Better sources to understand how portfolios can be used effectively has been Biggs' account, as well as independent experimentation with exercises and activities which can serve as portfolio items.

4.3. Overall summary

On the positive side, I am confident that I have established myself as a reflective practitioner, which clearly is a core objective in Biggs' book and in several PGCAP sessions. I am able to seek ideas and feedback from several sources, including students, colleagues, and literature, and my approach to teaching has continuously evolved over the last two years.

Through reflection, I have established my own approach and ethos for teaching, successfully incorporating both my own past experience and attitudes, and the core ideas from PGCAP. In my opinion this reflective practice is a key element of the requirements for distinction. I am not sure if it is a sufficient element.

Furthermore, I think it is clear that the quality of my modules has improved significantly since I started. There is still more to be desired, but I have the methodology to continue the improvement.

Teaching aside, I have had little profit from PGCAP. Because of the fragmentation, I don't have a good overview of what I was supposed to learn. Thus it is surprising to look at the expected learning outcomes, and see that it does not look terrible even on the non-teaching topics.

Looking at research, I have demonstrated that I have been rather successful. I already had an outstanding publication record when I started, and I have continued to receive acknowledgement for my qualifications during the last two years. Consequently, this has not been an area of priority. Fortunately, the benefits of reflective practice applies also

in research, so I consider myself well equipped to direct my own development when it is time to change focus.

In some cases, such as the session on 'Accountability', PGCAP has created the view that we are pawns in a game. This is quite contrary to the way Biggs strongly advocates that good teaching and good learning depends on individual effort more than anything else. This has made it clearly most rewarding to focus on teaching, but not so clear that this was the intention of the course.

Bibliography

[Big03] John Biggs. *Teaching for Quality Learning at University.* Open University Press, second edition, 2003.

[Com07] Andrew Comrie. Lectures for pgcap, 2006/07.

[Gib] G. Gibbs. Using assessment strategically to change the way students learn.

[Hol31] Ludvig Holberg. *Den Stundesløse.* 1731. Comedy in three acts (Danish).

[Kol84] D.A. Kolb. *Experiential Learning experience as a source of learning and development.* Prentice Hall, 1984.

[nsf97] Ledelse i nsf. Technical report, Norges Speiderforbund, June 1997. Norwegian.

[pgc07] Postgraduate certificate in academic practice (pgcap). Programme Handbook, 2006–2007.

[Ram03] Paul Ramsden. *Learning to teach in higher education.* RoutledgeFalmer, second edition, 2003.

A. Alter–Begin–Continue

A.1. Alter (red)

- avoid going off-topic for too long
- (2) split session in two
- two breaks (possibly shorter)
- more diagrams – ask students to draw diagrams
- less intense weekly exercises
- open discussion on exercises
- feedback on weekly exercises (BEGIN)
- more structure in peer review
- matrices seemed super-complicated
- reduce initial complexity of new topics; item express background in layman's terms before and after main topic
- (2) clearer wording in weekly exercises
- to much theoretical stuff
- more technical stuff (comp. science, not management)
- summary at the end of lecture
- more emphasis on key points

A.2. Begin (green)

- references to further reading in slides (where applicable)
- (2) examples of applications/implementations
- case studies from current industry

- more examples
- case studies, more practically oriented
- (2) provide «perfect»/full-format answers to some of the exercises solutions
- give standards for assignments
- maybe some practical exercises
- (2) live demos for as many topics as possible; e.g. show permissions in the unix system
- technical details (this feels like management type lecture)
- more maths and programming
- summary at the end of lecture
- fundamentals of computer security
- what occupations it can lead to

A.3. Continue (yellow)

- The course is very interesting
- Session structure : peer assessment + slides
- (6) Weekly Exercises
- Exercises incl. open discussion of answers
- Time enough for discussion
- (5) Discussion on exercises/feedback
- More interaction (group discussion)
- (5) Interactive lecture
- Group discussion
- Peer assessment
- with more exercises, discuss in class
- Flexibility of answers to questions
- 3h distribution : discussion + break + lecture

- Teaching style (keeps us awake)
- Good slide layout and detail
- Good structure: objectives + core + summary
- Clear slides : each is very good at highlighting a particular point
- fair discuss partner route
- more examples (BEGIN?)

B. Evaluation of CSM25 Spring 2007

How would you describe the workload in this module, compared to other modules?				
Much lower	lower	average *(2)*	higher *(6)*	much higher *(2)*
How much did you learn in this module compared to other modules?				
Much less	less	average *(2)*	more *(6)*	much more *(2)*
How relevant was your learning in view of your expectations?				
Highly irrelevant	Not satisfactory *(2)*	As expected *(2)*	Above expectation *(5)*	No opinion *(1)*
How did you find the organisation with lab exercises in the lecture classes?				
Strongly prefer dedicated lab session	Weakly prefer dedicated lab session *(3)*	No opinion *(1)*	Weakly prefer exercises in lecture *(3)*	Strongly prefer exercises in lecture *(2)*

How much did you learn from each of the learning activities?					
Lectures	Did not use	Almost nothing *(2)*	Less than satisfactory *(3)*	Satisfactory *(4)*	A lot *(1)*
Exercises	Did not use	Almost nothing *(1)*	Less than satisfactory *(3)*	Satisfactory *(4)*	A lot *(2)*
Coursework	Did not use	Almost nothing	Less than satisfactory *(2)*	Satisfactory *(4)*	A lot *(4)*
Web pages	Did not use *(1)*	Almost nothing	Less than satisfactory *(2)*	Satisfactory *(2)*	A lot *(5)*
Suggested reading material	Did not use *(1)*	Almost nothing	Less than satisfactory *(3)*	Satisfactory *(4)*	A lot *(2)*

Did you like the module as a whole?				
I wish I had taken another module	Not quite satisfied *(2)*	Satisfied *(3)*	Very pleased *(4)*	No opinion *(1)*

C. CSM27 Exercise Week 3

This is an example of a weekly exercise from CSM27, including the assignment, a student paper, and the formative feedback given.

C.1. Feedback

- *Problem 1.1*

  Very clear and readable answer. Nothing to be criticised.

- *Problem 1.2*

  The best thing about this answer is, in my opinion, that it is very structured, which makes it easy to read, and easy to check for consistency. The level of detail is above expectation, but this is just an advantage.

  If some additional effort is to be invested, it should be used to work on the rationale. The remarks at the end of D.4 is an example of giving a good rationale. The requirement to change password frequently could also require a similar disclaimer and argument.

  It is clearly an answer worthy of a distinction. With some extra effort on the rationale, I would place it in the 90-s.

  The other criticism is merely minor:

  – In Section D.1 Items 3-5, as a reader, I ask why. A brief comment and reference to Section D.4 where it is used, would be helpful

  – D.2 ref to film titles. Given this policy I suggest a dictionary attack based on film titles of 8-12 characters. If you give examples, the users will use them...

  – The ACC. The word code is ambiguous at best. Calling it a 'one-time password' would be less ambiguous. In my area, a code is always a set of words, and not a single word.

CSM27 Week 3
Identification and Authentication

Hans Georg Schaathun

November 30, 2007

1 Weekly Exercises

1.1 Gollmann 3.2

1. Assume that you are only allowed to use the 26 characters from the alphabet to construct passwords. How many different passwords are possible if a password is at most n, $n = 4, 6, 8$, characters long and there is no distinction between upper case and lower case characters?

2. How many different passwords are possible if a password is at most n, $n = 4, 6, 8$, characters long and passwords are case sensitive?

1.2 Security policy

- Draft a security policy for password management for student accounts at a university.
- Include security policy objective, and mechanisms for issuing new accounts/passwords and for reissuing passwords when one is forgotten.
- Give reasons for your choices.

2 Extra Exercises

The following exercises will not be assessed or discussed in session, but they are good, exam-relevant training.

2.1 From Gollmann Chapter 3

3.3 Assume that passwords have length six and all alphanumerical characters, upper and lower case, can be used in their construction. How long will a brute force attack take on average if it takes one tenth of a second to check a password? it takes a microsecond to check a password?

3.4 Assume that you are only allowed to use the 26 characters from the alphabet to construct passwords of length n. Assume further that you are using the same password in two systems where one accepts case sensitive passwords but the other does not. Give an upper bound at the number of attempts required to guess the case sensitive version of a password.

2.2 Your own system

- Consider the system on your laptops.
  - How are the passwords stored?
  - Can the adminstrator read user passwords?
  - In what way is the choice of password restricted?
  - Compare your system against the principles and suggestions in Gollmann, Section 3.3.

1.1 *Assume that you are only allowed to use the 26 characters from the alphabet to construct passwords. How many different passwords are possible if a password is at most **N**, **N = 4, 6, 8** characters long and there is no distinction between uppercase and lowercase characters?*

Assuming that each character from the alphabet can be used more than once, the different combinations of passwords possible is given by the following expression for the different values of ***N***:

When ***N*** = 4,

$= 26^1 + 26^2 + 26^3 + 26^4$
$= 26 + 676 + 17576 + 456976$
$= 475254$

When ***N*** = 6,

$= 26^1 + 26^2 + 26^3 + 26^4 + 26^5 + 26^6$
$= 26 + 676 + 17576 + 456976 + 11881376 + 308915776$
$= 321272406$

When ***N*** = 8,

$= 26^1 + 26^2 + 26^3 + 26^4 + 26^5 + 26^6 + 26^7 + 26^8$
$= 26 + 676 + 17576 + 456976 + 11881376 + 308915776 + 8031810176 + 208827064576$
$= 217180147158$

*How many different passwords are possible if a password is at most **N**, **N = 4, 6, 8** characters long and passwords are case sensitive?*

If passwords are case sensitive the number of combinations calculated in the previous workings would have to be doubled (there are now 52 characters in the alphabet), thus:

When ***N*** = 4,

$= 52^1 + 52^2 + 52^3 + 52^4$
$= 52 + 2704 + 140608 + 7311616$
$= 7454980$

When ***N*** = 6,

$= 52^1 + 52^2 + 52^3 + 52^4 + 52^5 + 52^6$
$= 52 + 2704 + 140608 + 7311616 + 380204032 + 19770609664$
$= 20158268676$

When $N = 8$,

$= 52^1 + 52^2 + 52^3 + 52^4 + 52^5 + 52^6 + 52^7 + 52^8$
$= 52 + 2704 + 140608 + 7311616 + 380204032 + 19770609664 + 1028071702528 + 53459728531456 = 54507958502660$

1.2 *Draft a security policy for password management for student accounts at a university.*

- *Include security policy objective, and mechanisms for issuing new accounts/passwords and for reissuing passwords when one is forgotten.*
- *Give reasons for your choices.*

A. Overview

Students at the University of Life are offered a range of services that can be accessed online, either from one of the desktop PC available on campus, or else through remote access from a PC external to the trusted local area network. The services available include the following:

- Personal file store
- Email
- Windows/Unix Lab service
- E-Learning scheme
- Library loan facilities
- One stop shop online

The students access all these services through a user account, which is provided to them when they enrol onto a course. Since these services contain confidential data, this account is password protected. This should allow only authorized users to view the relevant information.

B. Purpose

The purpose of this policy is to provide security guidelines and standards to all concerned parties for the following:

- Issuing a new user account and password
- Choosing the right password
- Protecting your password
- Changing or resetting a password
- Terminating a student account

C. Scope

The scope of this policy includes all administrative personnel responsible for the issuing of the user account password, as well as, the students whose responsibility is to follow the standards outlined in this policy.

D. Policy

D.1. Issuing a new user account and password

Once the student is offered a course, s/he will need to register with the university to acknowledge his/her interest in pursuing the studies. On successful registration, the university issues:

1. University Registration Number (URN)
2. Account Activation Code (AAC)

Both items are referred to as the Activation Material (AM) and are provided to the student through traditional mail, however, both are contained within a tamper-proof envelope.

On receipt of the Activation Material, the student accesses the University portal to activate his/her account. This is done by entering the Date of Birth (DOB), URN and the AAC. For a particular URN, the user has a grace allowance of up to 10 attempts to enter the correct combination. After that the activation process cannot be completed and a request for new AM should be made from the portal itself. The combination of the AM and the DOB reduces the probability of a student genuinely entering an incorrect URN/AAC pair, which happens also to be valid AM for another student. Furthermore, threats such as exhaustive attacks are controlled by the grace allowance and the large search space, which is made up from the composition of the DOB and AM.

On successful activation the student is presented with the following:

1. The user name to log on his/her account
2. Prompt to enter a new password for his/her account
3. Prompt to enter a secondary email address

4. Prompt to enter a local correspondence address and contact details
5. Prompt to answer a set of challenges

The student should enter a new password according to the guidelines in Section D.2 and ensure that the password is kept secret as outlined in Section D.3.

D.2. Choosing the right password

- The student account passwords should have a minimum of 8 characters and consist of a combination of uppercase and lowercase alphanumeric characters, as well as special characters.
- The password should be such that it would be easy to remember but difficult to guess. For instance, it can be the title of a favourite movie: CATch.M3.1f.Y0u.Can
- It should not be a word from a dictionary or a common usage word such as names of relatives, friends or pets.
- The password should not be in use for another account or system.

D.3. Protecting your password

- Passwords should never be written down on a piece of paper or in electronic format on a laptop, PDA or smart phone. Refer to Section D.2 on how to choose a password that is easy to remember but difficult to guess.
- Passwords should be changed periodically (possibly every month).
- Passwords should never be revealed to other persons, including administrative personnel responsible for password management.
- Passwords should never be sent by email or else revealed over the phone.
- Passwords should never be shared with anyone else, including friends.
- Do not use this same password for other accounts (e.g. ISP, Facebook, etc) or systems.

D.4. Changing or resetting a password

A student has the option to change his password from within the account itself. S/he can use this option anytime, including when:

- A suspicion arises that the password has been cracked
- The password has been revealed.

The system enforces the student to change the password periodically.

In case the student forgets the password, s/he has to make a request from the university portal to reset it accordingly. This can only be done after the student has successfully completed a series of challenges presented to him. The challenges can take up the form of questions or problems whose answer can only be known by the intended student, thus the authenticity of the request can be controlled.

If successful, the student will receive an activation link through the secondary email provided that will allow him to reset his/her password. If a secondary email is not supplied then the new password will be mailed in a tamper proof envelope to the alternative correspondence address provided. The presence of a Challenge-Response System and the secondary email account make it reasonably difficult for a third party to crack into the student account. It is understood that this method comprises a level of risk, however further measures would exceed the cost of the assets being protected, thus making it unreasonable to adopt.

D.5. Terminating a student account

When a student finishes his term at the university, then it is necessary to revoke access to the student account. The student is given a handover term of 15 days to clear any outstanding items on his part. On expiry of this term, the student account is disabled (for history purposes it is not purged from the system immediately) and password invalidated accordingly. This is necessary to allow only legitimate users to make use of the university resources.

E. Student Account Management Authority

Student accounts at the University of Life are managed solely by the IT – Staff & Student Section. For any queries or problems, the responsible personnel can be contacted on the following details:

Building SS Room 8
0900hrs – 1200hrs, 1300hrs – 1630hrs
Email: problems@life.ac.uk
Tel: 07912345678

F. Definitions

University Registration Number (URN) - The URN is a unique number that indexes the student on all university systems. This is a publicly known piece of information. The format of the URN consists of 3 alpha characters followed by 7 numeric characters.

Account Activation Code (AAC) - The AAC is a secret code that is used in the activation of the student account. This is a one-time code, which means that after it is used it is no longer valid. The format of the AAC consists of 8 numeric characters.

D. Formal Evaluation CSM25 2007

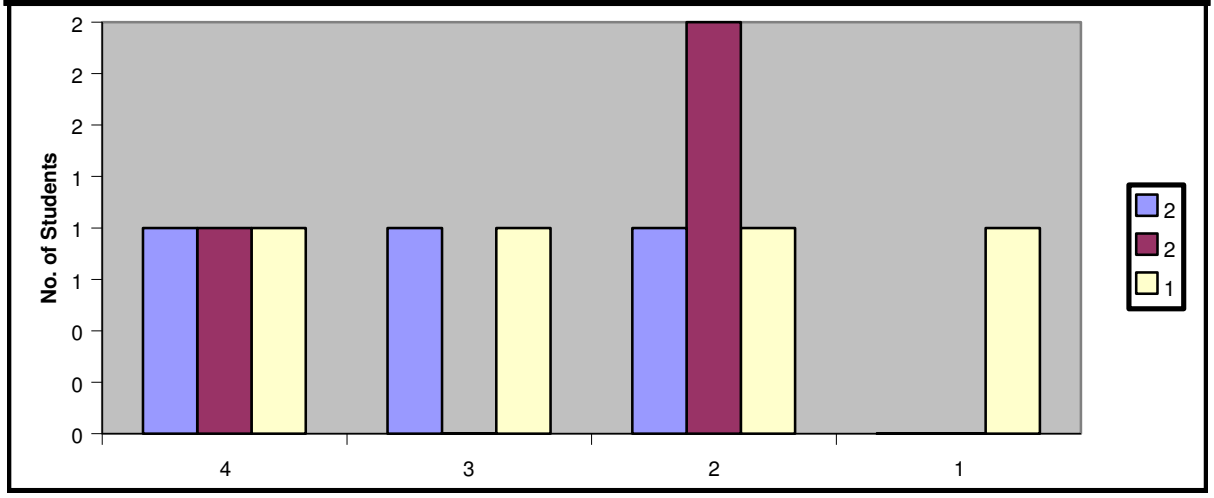
Department of Computing

SPRING SEMESTER 2007FEEDBACK
CSM25 Secure Information Hiding

Module Contact: Dr Hans George Schaathun

TOTAL STUDENTS = 5

	5	4	3	2	1		AVERAGE
Interesting	2	1	1	1	0	Boring	3.80
Well presented and delivered	2	1	0	2	0	Badly presented and delivered	3.60
Effective Learning Experience	1	1	1	1	1	Poor learning experience	3.00



Key:
5 - strongly agree with the left-hand statement
4 - partially agree with it
1 - strongly agree with the right-hand statement

Module Averages:

Course Interest	4.15
Presentation	3.95
Learning Experience	3.69

Comments:

Everything as very good.

UniS

University of Surrey
Module Report 2006-07

MODULE DETAILS

MODULE: **CSM25**

CONVENOR: Hans Georg Schaathun

LEVEL: M

CREDIT VALUE: 15

DELIVERY: **Spring**

TEACHING and ASSESSMENT: 60% Coursework 40% Exam

STUDENT PERFORMANCE

TOTAL NUMBER OF STUDENTS 13

MEAN MARK 60.2%

GRADE DISTRIBUTION

(80-100) **S**	(70-79) **A**	(60-69) **B**	(50-59) **C**	(41-49) **D**	(30-40) **E**	(0-29) **F**
0	1	7	4	1	0	0

PTO for Comments

COMMENTS BY CONVENOR

GENERAL COMMENTS:
The module is very specialised and the field rather immature. For instance, there was no adequate textbook. As this was not realised at the planning stage, there was insufficient time to develop the syllabus. The module was designed for STA and assumed that the students had technical background; it was not designed for the large number of IS students.

STUDENT FEEDBACK:
The official feedback included five replies with large spread.
The feedback I collected myself drew 10 replies, and also had significant spread. However it is clear that both the workload and the learning outcome of the module was above average. The majority of students were either satisfied (3) or very pleased (4).

ACTION POINTS:
1. No written exam; group-based and individual coursework.
2. More examples in slides and handouts. Make sample solutions.
3. Revise module outline, including lectures and exercises. Reduce the workload somewhat.
4. Consider new activities which can increase interaction in lectures.
5. Spend more time in class to discuss solutions to exercises.

Please complete this form and return it to the Postgraduate Office (29BB04) by 12.00 o'clock, Friday the 22nd June.

E. Formal Evaluation CSM27 2007

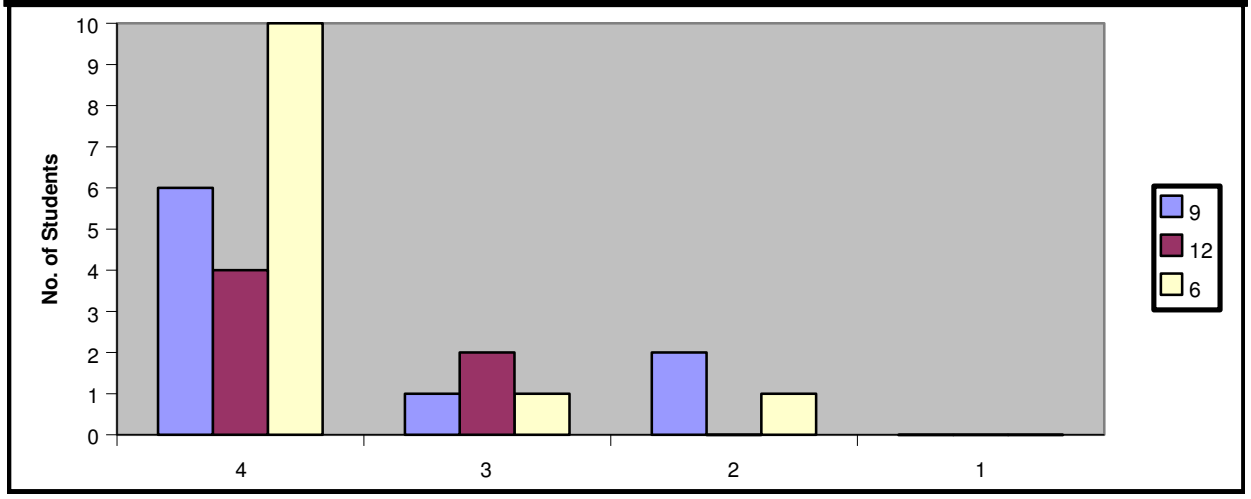
Department of Computing

AUTUMN SEMESTER 2007 FEEDBACK

CSM27 Computer Security
Module Contacts: Dr. Georg Schaathun

TOTAL STUDENTS = **19** RESPONSES = **18**

	5	4	3	2	1		AVERAGE
Interesting	9	6	1	2	0	Boring	4.22
Well presented and delivered	12	4	2	0	0	Badly presented and delivered	4.56
Effective Learning Experience	6	10	1	1	0	Poor learning experience	4.17



Key:
5 - strongly agree with the left-hand statem
4 - partially agree with it
1 - strongly agree with the right-hand state

Module Averages:

Course Interest	3.78
Presentation	3.57
Learning Experienc	3.48

Comments:
Very interesting and very well structured module.
I enjoyed this module because it was very interactive.
Excellent module very well delivered and taught.
Dr. Schaathun ensures that students achieve a good understanding of material.
Dr. Schaathun keeps course website up to date and gives regular feedback.

Module Report 2007-08

MODULE DETAILS

MODULE: CSM27 Computer Security

CONVENOR: Hans Georg Schaathun

LEVEL: M

CREDIT VALUE: 15

DELIVERY: **Autumn 2007**

TEACHING and ASSESSMENT: Coursework 30% Exam 70%

STUDENT PERFORMANCE

TOTAL NUMBER OF STUDENTS 19

MEAN MARK

GRADE DISTRIBUTION

(80-100) **S**	(70-79) **A**	(60-69) **B**	(50-59) **C**	(41-49) **D**	(30-40) **E**	(0-29) **F**
1	2	9	2 (3)	3	2 (1)	

Two cases of plagiarism. Numbers in parentheses are after resubmissions.

PTO for Comments

COMMENTS BY CONVENOR

GENERAL COMMENTS:
The grade distribution is not quite satisfactory.

STUDENT FEEDBACK:
Student feedback has been overwhelming, and they have particularly liked my scheme of weekly exercises.

ACTION POINTS:
Some polish is needed on the wording of exercises and assessment criteria to encourage the good reasoning. The coursework should next year be extended to include a short concluding essay, and its weighting correspondingly increased to 35% or 40%.

Please complete this form and return it to the Postgraduate Office (04AA02) by Friday the 22nd February.

F. Module Descriptions

Following are the module descriptions in the last version from my records. There has been a lot of problems in the publication and updating of the module descriptions. Changes were made administratively without consulting either the Board of Studies nor the module convenor, and old descriptions were republished without agreed updates. Thus I am unable to recover, at the moment, correct or official module descriptions.

Most blatantly, the exam/coursework weighting for CSM25 2006/07 is wrong. It should be 60% coursework and 40% exam.

Full Module Description, 2006/07

Module Title

Secure Information Hiding

Module Provider (AoU):	Dept. Computing	**Subject (3 letters):**	
Level:	M	**Number of Credits:**	15
Module Co-ordinator:	Dr. Hans Georg Schaathun		

Module Availability

Assessment Pattern

i) Unit(s) of Assessment	b) Weighting Towards Module Mark(%)
Coursework	50%
Exams	50%

Qualifying Condition(s)

An aggregate mark of at least 50%.

Pre-requisite/Co-requisites

CSM24 (Introduction to Multimedia Security)

Module Overview

Secure communications take different forms. Cryptography allows us to keep the contents of a message secret. Sometimes however, we need to hide the very existence of the secret message. This is known as steganography. The art of unveiling the hidden information in steganographic messages is called steganalysis.

There are at least two common approaches to steganography, one founded on cryptography and one developed from watermarking. This module will consider both of them, and study their strengths and limitations.

We will also look into different security paradigms. Kerchoff's principles have defined

cryptographic security for the last century, but they are rarely addressed in the watermarking communities. We shall try to answer why this is so, and provide an overview of the different notions of security. The students will learn how to assess security in a steganographic system, and have an overview of available methods of steganalysis.

Module Aims

The students will get an understanding of different notions of security; they will gain the practical skills to implement steganography systems, learn of typical methods of steganalysis, and obtain a general understanding of the general principles of steganography and steganalysis.

Learning Outcomes

The students will

- Get an overview of steganography, including approaches from cryptography and watermarking.
- Get practical experience with select systems of steganography.
- Get an overview of security paradigms.
- Learn to assess security in communications, and steganographic systems in particular.
- Learn about typical attacks against steganography.

Module Content

Steganography and data hiding, steganalysis, security paradigms.

Methods of Teaching/Learning

Lectures and coursework/labwork.

Selected Texts/Journals

Katzenbeisser & Petitcolas: *Information Hiding Techniques for Steganography and Digital Watermarking. (Subject to review)*

Peter Wayner: *Disappearing Cryptography (Subject to review)*

Module web pages, supporting material (TBA).

Date Last Revised: Draft 20 April 2006

Full Module Description, 2007/08

Module Title
Secure Information Hiding

Module Provider (AoU)	Dept. Computing	**Subject (3 letters)**	COM
Level	M	**Number of Credits**	15
Module Co-ordinator	Dr. Hans Georg Schaathun		

Module Availability

Spring

Assessment Pattern

i) Unit(s) of Assessment	**b) Weighting Towards Module Mark**
Poster on a chosen topic from the module (Group coursework, collective mark)	25%
Poster presentation (individual mark based on verbal presentation and own contribution)	25%
Individual coursework (9-10 weekly exercise sheets are given and discussed in class; 5 (random) sheets are requested and assessed in an end-of-term assessment)	50% (10% per sheet)
Qualifying Conditions(s) An aggregate mark of at least 50%	

Prerequisites/Co-requisites

CSM24 (Introduction to Multimedia Security)
CSMxx (Computer Security)

Module Overview

Secure communications take different forms. Cryptography allows us to keep the contents of a message secret. Sometimes however, we need to hide the very existence of the secret

message. This is known as steganography. The art of unveiling the hidden information in steganographic messages is called steganalysis.

There are at least two common approaches to steganography, one founded on cryptography and one developed from watermarking. This module will consider both of them, and study their strengths and limitations.

We will also look into different security paradigms. Kerchoff's principles have defined cryptographic security for the last century, but they are rarely addressed in the watermarking communities. We shall try to answer why this is so, and provide an overview of the different notions of security. The students will learn how to assess security in a steganographic system, and have an overview of available methods of steganalysis.

Module aims

The aim is to enable the students to assess security and security needs in communications with a critical view, and to equip them with knowledge to propose solutions for steganography and steganalysis.

Learning outcomes

By the end of the module, the students should

- be able to implement simple stego-systems based on data hiding.
- be able to implement simple steganalytic techniques.
- contrast the wide range of different views on, models for, and techniques for steganography.
- be able to critically review security in proposed communications systems in general and in steganographic techniques in particular.

Module content

- Introduction to steganography
- Principles for Secure Communications
- Steganography by image data hiding in the spatial domain
- Statistical Steganalysis

- Steganography and steganalysis in the transform domain (JPEG)
- Steganography from a cryptographic point of view
- Steganography without data hiding

Methods of Teaching/Learning

- 3-hour session every week for ten weeks (lectures integrated with lab work using laptops)
- Weekly exercises to be completed between sessions and peer-assessed during session.
- Mandatory poster sessions in Week 11-12 where group coursework is presented to the class and examiners

Selected Texts/Journals

No suitable core textbook is available on the market at the time of writing. If a suitable textbook is published in time for the module, it may be added as essential reading later.

The students should pay attention to the module web pages, and details about further suggested reading material will be published there.

Recommended reading

[1] Michael Backes and Christian Cachin. Public-key steganography with active attacks. 3378, 2005.

[2] Jessica Fridrich, Miroslav Goljan, and David Soukal. Higher-order statistical steganalysis of palette images. In *Proc. SPIE Electronic Imaging*, pages 178–190, January 2003.

[3] S. Katzenbeisser and F. A. P. Petitcolas, editors. *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, 2000.

[4] Niels Provos and Peter Honeyman. Hide and seek: An introduction to steganography. *IEEE Security and Privacy*, May/June 2003.

[5] Peter Wayner. *Disappearing Cryptography*. Morgan Kaufmann Publishers, 2nd edition, 2002.

Supplementary reading

[6] Gouri K. Bhattacharyya and Richard A. Johnson. *Statistical Concepts and Methods.* Wiley.

[7] Rafael C. Gonzalez, Richard E. Woods, and Steven L. Eddins. *Digital Image Processing using Matlab.* Pearson Prentice Hall, 2004.

Last Updated

May 30, 2008

Full Module Description, 2007/08

Module Title
Computer Security

Module Provider (AoU)	Dept. Computing	**Subject (3 letters)**	COM
Level	M	**Number of Credits**	15
Module Co-ordinator	Dr. Hans Georg Schaathun		

Module Availability

Autumn

Assessment Pattern

i) Unit(s) of Assessment	**b) Weighting Towards Module Mark**
Written, unseen examination (answer two out of three questions)	70%
Individual coursework (9-10 weekly exercise sheets are given and discussed in class; 3 (random) sheets are requested and assessed in an end-of-term assessment)	30% (10% per sheet)
Qualifying Conditions(s) An aggregate mark of at least 50%	

Prerequisites/Co-requisites

None

Module Overview

Security is probably the greatest challenge for computer and information systems in the near future. Many users have lost data due to viruses, both on home and business computers. Most of us have seen a range of email messages attempting different kinds of fraud. Security holes can potentially affect all of us, from innocent home users to

complex corporate systems. Internet banking and e-commerce means that money is at stake, even for common people.

This module will explain some central security models and frameworks, which will be further illustrated by case studies where we get experience with real-life security problems.

Module aims

The aim of the module is to equip the students with knowledge and theoretical skills to assess security in large systems and to incorporate security in the design process.

Learning outcomes

At the end of the module, the students will

- understand and be able to use formal models for computer security
- be aware of the many security pitfalls at the various stages of systems development
- be able critically to review security at each stage of the development process

Module content

- Foundations of Computer Security
- Identification and Authentication
- Access Control as a Case Study
- Formal Models, including
  - State Machine Modles
  - Bell-LaPadula Model
  - Chinese Weall Model
- Security Evaluation
  - Evaluation methodology
  - The Orange Book

- Software Security
  - Input checking
  - Broken abstractions
  - Memory management and buffer overflows

Methods of Teaching/Learning

- 3-hour session every week for ten weeks (lectures integrated with lab work using laptops)
- Weekly exercises to be completed between sessions and peer-assessed during session.

Selected Texts/Journals

Essential reading

Recommended reading

- *IEEE Security and Privacy* (magazine)

Pay attention to module web pages for additional reading recommendations.

Supplementary reading

Last Updated

May 30, 2008

G. Peer observation

Postgraduate Certificate in Academic Practice
Peer Partner Teaching Observation Form

FORM A – PREPARATION

To be completed by the Observee and forwarded to your Peer Partner at least 1 week prior to the observed session

Name Hans Georg Schaathun **School/Dept Computing**	**Observer Henriette Høgh**	**Date 21/02/2007** **Time 10-11**
Nature of session Class (e.g. lecture, seminar etc.)	**Level Masters**	**Venue TB19**
Title of the Module CSM25 Secure Information Hiding **Title of session The DCT domain and JPEG**		

Intended student learning outcomes

Have an overview of JPEG compression works, and the image representation formats used.
Be able to implement JSteg embedding, including conversion from spatial representation to DCT representation.

Session plan
Outline the structure of session, brief indication of content and the learning and teaching strategies to be used

1. Recap from last session. Ask each student for one interesting point learnt and one question.

2. Give an overview of JPEG compression and the transform domain as a lecture, interrupted by short computer exercises.

3. Give a second lecture to
   A. Explain how the known techniques of LSB embedding can be applied to the JPEG representation
   B. Present a series of improvements to the LSB embedding (Outguess, F3, F4, F5)

4. If time, start on lab exercise; implement JPEG-based embedding techniques in Matlab.

How does the session relate to previous and subsequent taught sessions or learning activities?

It assumes that the students have implemented steganography and –analysis in the spatial domain from previous lectures and exercises.
Mandatory coursework will focus on the implementation of techniques covered in this session.
A quick introduction to matrix coding and applications of coding theory to minimise distortion was introduced. Elaborating theory follows two weeks later.

Apart from this, there is little relation with subsequent lectures. This session is the last in a series of sessions intent to enable the student to implement simple systems. Of course, the hands-on experience from the exercises is hoped to give them a better appreciation of theory covered later.

How do the aims and learning outcomes of the session relate to the learning and teaching strategies adopted?

One of the prime learning outcomes is to be able to implement simple systems, and this is the session focuses on some selected systems.

What do you hope to learn from this session that will aid your development as a teacher?

I seek a second opinion on how the interleaving of exercise and lecture work in practice, and also how questions to the audience work.

Frankly, I do not have time to consider how to teach this term, as all available time is spent on what to teach.

Identify any areas or issues you would specifically like to receive feedback on from your Observer

- **Use of discussions and exercises during lecture**
- **Driving the dialoque**

FORM B (PART I) – OBSERVATION FEEDBACK

To be completed by the Observer following the observation and forwarded to the Observee preferably within 1 week or as soon after as possible for discussion

Comment on the strengths and identify aspects for development or improvement in relation to:

Strengths:

- **Good to start with short exercise to 'break the ice' and encourage students to interact**
- **The follow to questions and answers, i.e. 'did that answer your question' and 'is that the answer you were looking for?' as this helps clarify the problem/solution**
- **The mixture of exercise and lecture, as this breaks the high level of concentration needed during the lecture bit, and completion of the exercise ensures the students have understood what have just been covered**

Improvements:

- **Give expected time scale for larger exercises?**
- **Maybe try and have some of the exercises done in pairs rather than alone, as this will encourage peer interaction, and also might help students more freely or willingly interacting with teacher (as some students may not seek help, due to language difficulties/lack of confidence in language skills)**

Please direct your comments mainly to the following three areas;

Support of student learning

(e.g. awareness of student learning processes; promotion of active learning; identification of learning needs including equal opportunities issues; monitoring and evaluation of student learning)

Learning activities

(e.g. defining of learning outcomes and links with learning and teaching activities; use of a range of appropriate learning and teaching activities; coherence of structure and organised development of student learning; opportunities for student interaction and participation or development of student autonomy)

Teaching activities

(e.g. session management; use of a range of educational support materials appropriate to the learning context; use of effective verbal and non-verbal communication)

- **Good monitoring of student learning through exercises**
- **Learning outcomes could be specifically stated at beginning of lecture or in the handout**

Observation feedback continued

Feedback on areas or issues specifically requested by the Observee

- **As discussed, students no very active in dialogue, but not sure how to improve on this**
- **Exercises seemed to work well at achieving a deeper level of knowledge**

Further comments or issues on observed session (including suggestions for improvement if any). On the more practical aspects of delivery you might feel it appropriate to comment upon some or all of the following:-
Methods used for the session, i.e. handouts, overheads, chalk, PowerPoint, lab. Instructions, etc. and their clarity and effectiveness.
Manner of delivery, too fast, too slow, audibility etc..

- **Speed of deliverance good**
- **Audibility good**
- **Powerpoint presentation clear**
- **Good control of room and confidence in lecturing and helping during exercise**
- **Presentation overall seemed well prepared**

FORM B (PART 2) – REFLECTION & EVALUATION

To be completed following discussion between the peer partners

What are the most important issues raised by the feedback from your Observer?

- **Think about ways of increasing interaction between students and with lecturer**

Agreed action points

To be agreed by the Observee and the Observer

- **Evaluate/more careful phrasing of problems based on own solution**
- **Incorporate more group work**

Observer's Signature	
Observee's Signature	
Date	

H. Poster topics

H.1. Proposed topics which were used

- Consider steganography by mimicry using grammars, as described in Wayner's book and implemented at `http://www.spammimic.com/`. Is it a secure? Is it practical? You can (for instance) either (1) evaluate the idea, possibly by implementing and testing it yourselves, or (2) evaluate the spammimic.com web site.
- Give an introductory overview to coding theory and its relations to steganography, adding some interesting detail beyond the coverage from my lectures.
- Make a literature survey on applications of steganography and steganalysis in 'terrorist' organisations and intelligence services. Assess the significance of the field in terms of national security. You should make an extensive literature search, but avoid technical detail.
- *What is randomness?* Such an apparently simple question can be quite controversial and philosophically challenging. The project should browse the literature for a range of opinions about and attempts to define randomness. Subsequently, these findings should be interpreted and summarised with a view to applications in steganography.
- In principle LSB and other spatial stego-techniches by modification apply also to palette images (e.g. GIF), but there are certain problems. Explain what palette images are, and discuss how steganography by modification can be performed. It is a good idea to base the disussion on own implementations and tests.

H.2. Topics proposed by students

- Industrial espionage and watermarking/fingerprinting integrated in printers.
- Steganography in audio files.