Development of a Masters module in Computer Forensics and Cybercrime

Richard E Overill

Department of Computer Science, King’s College London, The Strand, London, WC2R 2LS, UK

Abstract
In mid-2004 it was decided that the list of optional modules available to students taking the MSc programme in Computing, Internet Law and Management at King’s College London should be supplemented with a module in Computer Forensics and Cybercrime. It was proposed that this module should be delivered as a reading course to be assessed by means of a dissertation and a linked viva voce examination.

We trace the evolution of this module over the three academic years 2005/6 to 2007/8 inclusive and discuss the range of dissertation topics selected by the students. The results obtained by the students and the evidence from anonymous student feedback surveys are analysed quantitatively. We conclude with a critical assessment of the success of the module in meeting its specified aims and objectives and put forward proposals for its future development.

Introduction and Background
The MSc programme in Computing, Internet Law and Management (CILM) is one of four MSc programmes in Computer Science currently offered by King’s College London (KCL) and it is the only one that can be taken in either full-time or part-time modes of study. Teaching of the Internet Law and Management components has until now been subcontracted to the School of Law and the Department of Management respectively. In mid-2004 it was decided to enhance the portfolio of optional Computing modules on offer to the MSc CILM students by the addition of a module entitled Computer Forensics and Cybercrime (code: CSMCFC)[1].

The stated aim of the module is “to provide students with a solid foundation to understand the concepts involved in both computer forensics and cybercrime”. Its learning outcomes are defined as follows: “At the end of this module a student is expected to understand computer crime, together with its social and legal implications; understand the techniques for computer and network forensics; understand, and relate the above points to, the UK Computer Misuse Act and related EU legislation”[2]. A significant feature of this module is that it is not delivered as a formally examined lecture course or as a laboratory-based course. Rather, it was decided that it should be offered as a reading course to be assessed by means of a written dissertation and an accompanying oral presentation to the assessors. This would also bring the MSc CILM into line with the other three full-time MSc programmes for which a dissertation based optional module entitled Advanced Research Topics (code: CSMART) was already available.
In the following sections we discuss the range of dissertation topics selected by the students, we analyse quantitatively the results obtained by the students over the past three successive academic years, and we evaluate the anonymous student feedback obtained via the standard KCL module evaluation MCQ. We conclude the paper with a critical assessment of the degree to which the published aims and objectives of the module have been successfully achieved, and some comparisons with the results of our previous studies in this area.

**Dissertation Topics**

Students are free to select any dissertation topic in consultation with the module leader whose main functions are to ensure (a) that each topic selected clearly falls within the scope of the module; and (b) that the topic does not overlap significantly with those topics already selected by other students. The topic selection process is preceded by an induction meeting at which the module leader outlines the scope of the module, indicates the principal resources available for research, and explains how the dissertation and presentation are to be assessed. The list of dissertation topics selected by the students over the past three years is shown below; the four topics that were selected more than once in different academic years are marked (2): one topic was ultimately ruled out-of-scope.

- Computer related crime: hackers, malware and spyware
- Computer assisted crime: financial fraud, embezzlement and blackmail
- Social engineering and cognitive hacking
- Cyber-squatting (2)
- Trojan horses (2)
- Phishing attacks
- Commercial espionage and sabotage
- Biometrics: fingerprint analysis
- DNA cryptography
- Digital IPR and music piracy
- Cyber-stalking (2)
- Anti-forensics
- Virtual crime
- Cognitive hacking pump-and-dump schemes
- Computer virtualisation in forensic investigations
- Scams by cyber-criminals
- Motivation of malware creators (2)
- Virtual crime
- Trends in cyber-warfare and national security in the Internet age
- E-banking fraud

While only two of the above topics are explicitly concerned with cyber-forensics *per se* the remainder are implicitly linked to it via the traces that may be left at the scene-of-crime. The apparent imbalance in topic selection reflects the profile of the student intake to the MSc CILM programme where the part-time students almost without exception held full-time information security management posts and many of the full-time students held Bachelors degrees with a strong Law or Management component. Only those full-time students holding single honours Computer Science BSc would be likely to consider the possibility of selecting a dissertation topic explicitly concerned with cyber-forensics.
Analysis of Results

The dissertation assessment scheme can be summarised as follows: A thorough literature review covering the whole topic is normally awarded a Pass. In addition, a rigorous critical analysis, assessment and evaluation of the selected topic is normally awarded Merit. Further, an original proposal or novel contribution to the selected topic is normally awarded Distinction. The recommended dissertation length is 3000 words. All student dissertations were independently double marked and the individual marks were then reconciled and ranked by three assessors working as a team. Internet search engines were routinely employed to look for evidence of direct plagiarism in all the dissertations; the students were pre-warned of this. Where a topic had been selected previously, the electronic copy of the previous dissertation was also checked. The results so obtained are displayed in the Table below (Pass = 50+; Merit = 60+; Distinction = 70+):

<table>
<thead>
<tr>
<th>AY</th>
<th>#Stdts</th>
<th>#F/T</th>
<th>#P/T</th>
<th>#Fail</th>
<th>#Pass</th>
<th>#Merit</th>
<th>#Dist</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005/6</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>58.0</td>
</tr>
<tr>
<td>2006/7</td>
<td>12</td>
<td>10</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>57.1</td>
</tr>
<tr>
<td>2007/8</td>
<td>10</td>
<td>10</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>59.8</td>
</tr>
<tr>
<td>Overall</td>
<td>25</td>
<td>20</td>
<td>5</td>
<td>2</td>
<td>12</td>
<td>8</td>
<td>3</td>
<td>58.3</td>
</tr>
</tbody>
</table>

While the year-on-year trend for average mark is essentially constant at a high Pass, the overall category profile reveals 12% Distinctions, 32% Merits, 48% Passes and 8% Fails. This shows that although the students self-selected their dissertation topics they nevertheless found it challenging to perform the task at advanced Masters level.

Student Feedback

The standard KCL module evaluation MCQ contains twelve positive statements about the delivery and content of the module to each of which all students taking the module are encouraged to respond with one of five responses ranging from strong disagreement, through undecided, to strong agreement. The students’ responses to the statements are gathered anonymously at the end of the module and then only if more than three students are taking the module. Students also have the option to append a freehand comment to the MCQ. In fact, four of the statements are inapplicable to a reading course and these were therefore removed from the MCQ. The results of the survey (in the form of percentages) are displayed in the Table below:

<table>
<thead>
<tr>
<th>Statement</th>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Undecided</th>
<th>Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>50</td>
<td>40</td>
</tr>
<tr>
<td>B</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>30</td>
<td>70</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>50</td>
<td>40</td>
</tr>
<tr>
<td>D</td>
<td>0</td>
<td>0</td>
<td>20</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>F</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>40</td>
<td>50</td>
</tr>
<tr>
<td>G</td>
<td>0</td>
<td>0</td>
<td>30</td>
<td>30</td>
<td>40</td>
</tr>
<tr>
<td>J</td>
<td>0</td>
<td>0</td>
<td>20</td>
<td>30</td>
<td>50</td>
</tr>
<tr>
<td>L</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>40</td>
<td>60</td>
</tr>
</tbody>
</table>

A standard measure of overall student satisfaction (MOSS) is to take the ratio of the number of responses in the Agree/Strongly Agree categories to the total number of responses. In this case we obtain a MOSS value of 0.875, which equates to a student
satisfaction rating of 87.5% for the module. The sole freehand student comment on the module is perhaps worth quoting *verbatim*: “Great course. Dr Overill is friendly, knowledgeable and approachable. I was a little concerned at first about unclear requirements but the lecturer clarified. You get what you are willing to put into the course”.

**Summary and Conclusion**

The results presented in this paper can be compared with those from two previous quantitative studies in which a cyberforensics based curriculum is delivered to MSc students of Forensic Science and to MSc students of Computer Science.[3,4] The average percentage marks (rounded to the nearest integer) for each of these four MSc programmes are collected together in the Table below:

<table>
<thead>
<tr>
<th>Programme</th>
<th>Institution</th>
<th>#Years Data</th>
<th>Assessment</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSc For.Sci.</td>
<td>KCL</td>
<td>7</td>
<td>Examination</td>
<td>51</td>
</tr>
<tr>
<td>MSc For.Sci.</td>
<td>U.Strathclyde</td>
<td>4</td>
<td>Exam. + Lab.</td>
<td>55</td>
</tr>
<tr>
<td>MSc For.Inf.</td>
<td>U.Strathclyde</td>
<td>4</td>
<td>Exam. + Lab.</td>
<td>53</td>
</tr>
<tr>
<td>MSc CILM</td>
<td>KCL</td>
<td>3</td>
<td>Dissertation</td>
<td>58</td>
</tr>
</tbody>
</table>

The rather higher average mark for the dissertation based mode of assessment is not entirely unexpected; conversely, the slightly lower average mark for the examination only mode of assessment is indicative of the influence of time pressure on the students’ performance.

Perhaps somewhat surprisingly, the adoption of a reading course format for a Masters level module in computer forensics and cybercrime, assessed by means of a self-selected dissertation of 3000 words and an accompanying oral presentation, has proved remarkably successful in fulfilling the stated aims and objectives of the module. This is due in some measure to the fact that the students are able to tailor the module to their own individual interests. To avoid the module becoming too narrowly focussed all students are expected to attend all the presentations. Students are also encouraged to visit the module leader for informal one-to-one on-demand mini-supervisions of about 30-60 minutes’ duration during the selection, planning and writing of their dissertation. It is noticeable that the students who make sensible use of this facility tend to be those who obtain better marks.

The module has recently been transferred into the core module set for the MSc CILM at KCL and is also designated a core module for a new MSc in Computing and Security commencing in 2008/9. Finally, as a result of feedback from some students with a specific interest in cyber-forensics, it is planned to make a bid to the KCL Teaching Strategy Fund to establish a small cyber-forensics laboratory in order to give such students the opportunity to gain some hands-on experience in this increasingly significant discipline.

**Acknowledgement**

The author gratefully acknowledges Dr Ian Ferguson (University of Strathclyde) for the data taken from reference [4].

**References**
[1] CSMCFC Computer Forensics and Cybercrime module webpage: 
http://www.dcs.kcl.ac.uk/local/teaching/units/material/csmcfc/

[2] CSMCFC Computer Forensics and Cybercrime module syllabus: 
http://www.kcl.ac.uk/content/1/c4/92/11/CIMstructuremodules8.pdf

http://www.dcs.kcl.ac.uk/staff/richard/CFET_2007.doc

http://www.dcs.kcl.ac.uk/staff/richard/HEA-ICS-TchCompFor_paper.pdf