12

A Taxonomy and Overview of Information Security Experiments

E. Jonsson
Department of Computer Engineering
Chalmers University of Technology, S-412 96 Göteborg, Sweden
T: +46 31 772 1698, fax:+46 31 772 3663
email: erland.jonsson@ce.chalmers.se

L. J. Janczewski
School of Business and Economics, The University of Auckland
Private Bag 92 019, Auckland, New Zealand
T: +64 9373 7599, fax:+64 9373 7430
email: l.janczewski@auckland.ac.nz

Abstract

In July 1995 the Erasmus Bureau published a review of university programmes on Information Security followed by a proposal for an Information Security curriculum. These publications represent the first systematic attempt to review the Information Security discipline and to develop a common university program in the arena. The aim of the research presented in this paper is to bring this work one step further by means of surveying and systematising the role of experiments and practical project work in the discipline. We have thus made a world-wide inquiry to gather information on existing experiments. A few of these are presented in some detail, to give the reader a feeling for what is available. Furthermore, on the basis of the replies, we suggest a taxonomy for such experimentation and we classify the existing experiments accordingly.

Keywords

Security, experimentation, education, action learning, classification, taxonomy.

1 INTRODUCTION

In July 1995 the Erasmus Bureau published a review of university programmes on Information Security (ERASMUS 1995) followed by a proposal for an Information Security curriculum (ERASMUS 1995b). This set of publications is very important as it is the first systematic attempt to review the discipline and develop a universally accepted university program in the Information Security arena. For obvious reasons such publications do not define the delivery methods. It seems logical that the research phase to follow the set of ERASMUS publications should deal with the method of delivering the Information Security topics. An analysis of the ERASMUS project's publication (ERASMUS 1995) brings us to several quite interesting conclusions. One is the following:

The review of the existing programmes in the field was based mainly on what is offered at one Australian and seven European universities. It shows that these universities are using over 140 different textbooks. Among the publications listed, only one textbook, (Pfleeger 1989), is used at four institutions, one publication, (Muftic 1989), at three locations and 12 publications are used at two universities. The rest of the texts are limited to only one university institution. It is obvious that at the present there is not a great deal of coordination or exchange of information about contents and method of delivery of Information/Data Security subjects. Research on some aspects of delivery methods would be useful.

Therefore, during the 1996 IFIP SEC'96 conference, the IFIP WG 11.8* discussed an interesting topic: to what extent is the data security education at university level supported by practical activities, demonstrations, experiments or projects? This discussion, along with the other factors above, became a launching pad for this research, which discusses the possible ways of enhancing Information/Data Security presentation with practical experiments. The present paper covers the rationale behind conducting the experiments, introduces a classification of experiments and lists examples of experiments that might improve the quality of the teaching of the subject.

In the following, section 2 explains the scope of the topic and section 3 gives a framework for the experimental approach. The aim of the research presented is to systematise the role of experiments in teaching data security topics. Such a subject can not be dealt with without presenting experiments already introduced by various university organisations. We therefore contacted about 30 universities on five continents and asked about the contents of such experiments. The result is summarised in section 4. A brief evaluation of the data is made in section 5, and section 6 suggests possible directions for future work. Section 7 concludes the paper.

2 SCOPE

2.1 The action learning approach

In recent years there has been a growing interest in the *action learning* approach to education. Since 1990, International Congresses on Action Learning, Action Research and Practical Management (Brisbane 1990, Brisbane 1992, Bath 1994, Bogota 1996) have been held on this topic every two years, where scholars from all over the world discuss this approach to education.

---

* Working group WG 11.8 operates under the auspices of the Technical Committee TC11 of IFIP and concentrates on issues of data security education.

According to (Revans1992), (Revans 1984), action learning is a process by which groups of people (whether managers, academics, teachers, students or 'learners' generally) work on real issues or problems, carrying real responsibility in real conditions. The solutions they come up with may require changes to be made in the organisation and they often pose challenges to senior management, but the benefits are great because people actually own their own problems and their own solutions (Zuber-Skerritt 1990).

The action learning approach seems to be ideally suited to studying data security problems. While this discipline does have some highly theoretical parts (such as cryptography), in the majority of cases data security issues are very practical, and are implemented in the real life situation by the developers themselves.

Action learning is based on the Experiential Learning Cycle develop by (Kolb 1994). See Figure 1.

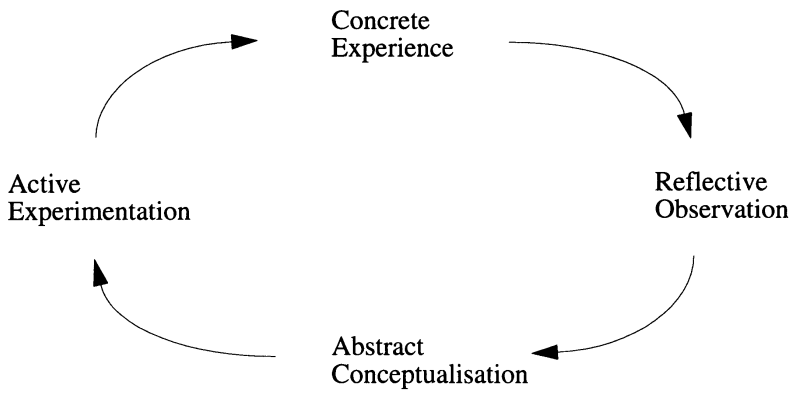

Figure 1 The Experimental Learning Cycle.

This cycle indicates the importance of active experimentation, and as a logical extension, significant parts of data security teaching should be based on experimental learning.

2.2 Difficulties with security experimentation

There are several reasons why conducting experiments in the field of data/information security is difficult. The discussion below gives the most important factors supporting that statement:

Information/data security is a rapidly changing discipline. In most cases experiments require lengthy preparation and academics investing great effort in preparing them wish to run them for several years. In the case of data security, this is almost impossible. On the contrary, the development of an experiment increases the effort required to deliver the topic. A good example would be the issue of viruses. Almost all dogmas about them have been changed in recent years. For instance, the arrival of macro viruses invalidated the well known statement that viruses are

limited to one platform, i.e., PC viruses do not spread into the Mac world and vice versa. Hence preparation of a demonstration on virus properties requires a careful following of developments in this field and proper updating of the experimental content every year.

Data security experiments generally deal with very sensitive issues. A data security experiment may reveal weak spots in the security armour of an organisation and it might be used against an organisation in many ways: through direct attack or public exposure. Business organisations are well aware of that, and a great deal of persuasion is usually necessary to involve them in a data security experiment. Some time ago, when the issue of data security was relatively new, participants were generally more eager to be involved than they are today. In 1991 the University of Auckland conducted a survey of data security arrangements among local community enterprises. Approximately one hundred organisations were approached and the response rate was 56%. The same research group wished to perform a follow-up of that survey in 1995. Unfortunately the project had to be abandoned, as the response rate was about 5%(!). It was clear that Auckland's business community was alien to this research.

Data security research, by definition, probes the proper functioning of a system. Thus it may happen quite often that an experiment that is "successful" from a researcher's point of view may have quite a disastrous results on an evaluated system. For example, students examining the efficiency of a password system may accidentally gain access to sensitive data or suspend the functioning of the whole system by their actions. Data security experiments should be well protected against these types of calamities.

2.3 Legal issues

Apart from being familiar with technical problems, a data security researcher should be aware of the legal problems resulting from the experiments he/she is conducting. Legal problems focus on the possible violation of privacy laws or similar legislation. An example would be: during a workshop on eavesdropping techniques the students tap highly confidential information. Using that data for any purpose outside the data security research is, of course, forbidden. However, in many countries, permission must in any case be obtained to listen or tap such transmissions.

3 A TAXONOMY FOR SECURITY EXPERIMENTS

Under the terms of this research, an *experiment* is defined as any activity which is outside the typical lecturing environment, in which a lecturer tells the audience about the theory or practice of the subject. This section suggests a classification of such experiments along three axes: *degree of applicability, degree of innovation* and *level of generalisation.* These are explained in the following.

In terms of ***degree of applicability,*** or distance from reality, the experiments may be of three types, denoted *D, L* and *F,* for *DEMONSTRATION, LABORATORY* and *FIELD WORK,* respectively.

D. Conducted by the staff (DEMONSTRATION).

This type of experiment assumes the audience to have a passive role. The lecturer or guest speaker demonstrates the practical side of the addressed course item being addressed. For instance, a lecturer would present (during a lecture) the practical functioning of the reference

monitor by connecting to a server and demonstrating various access rights. This type of presentation might take place at any location: it could be arranged during lecturing time, during a session in a university laboratory or at a real business/industrial organisation.

The common denominator is the same: students are passive and demonstrators are active during the conducting of the experiment.

L. Conducted by students in an artificial environment (LABORATORY)

This type of experiment assumes that the students have an active role and are asked to investigate a problem by themselves. The role of the staff is to explain the background, help in case of difficulties etc., but to stay away from the actual experiments. Experiments might be aimed at confirming some theoretical aspects of information security, for instance investigation of the time required for encryption/decryption of a text, or to solve some practical problem, for instance design of an access mechanism.

F. Conducted by students in the real environment (FIELD WORK)

Field Work experiments assume that students are asked to study a problem in a real-life organisation. Such an activity might, for instance, be investigation of the perimeter controls or design of a data security policy for an existing organisation.

The above classification is based on the distance between the participants, i.e., students, and the reality investigated; from a totally passive role (DEMONSTRATION) to dealing with very real problems (FIELD WORK). It implies that DEMO exercises could generally be presented without special preparatory work by students, while FIELD WORK is impossible without that.

The second way to classify experiments is to evaluate the ***degree of innovation*** of the ***object(s)*** of a particular activity. Examples of objects are hardware and software tools, mechanisms, protocols, set of rules etc. The most general classification would include the following classes:

U. Use of the object

These exercises are confined to normal use of the object. The goal might be to learn how it functions and in what situations it could be utilised. An example would be a lecturer that, during a class, is using an authentication and verification procedure to access the system in question.

E. Evaluation of the object

Here the exercises are aimed at presenting the object of the existing information security systems in such a way that its function and use can be evaluated and perhaps rated against other similar objects. A good example of such an activity would be a data security audit.

R. Redesign of an object

The purpose of these experiments is to make a new design of an existing object in order to learn about its basic functionality. The intended result is a better understanding of the security problems related to the design of the object as well as to the integration of it into its intended environment.

N. Design of new or improved objects

These exercises are the most difficult in the classification system. They require in-depth knowledge of the problem area investigated, which could result in new, improved designs of existing objects or recommendations aimed at enhancing the security of the installation. In more advanced cases, this class would also include the development of entirely new (and hopefully more secure) objects.

A step from the U to the N class requires an increased amount of knowledge in and experience of the domain.

The final way of classifying experiments is to define their ***level of generalisation.*** At this stage, we suggest the introduction of three classes:

M. Managerial level

Experiments of this class deal with an overall, organisational level of data security issues. A data security audit of a business unit, as mentioned before, may be example of such an activity. Security policy issues also belong to this level.

S. System level

This is the level of the system administrator as well as the level of abstraction experienced by the normal user of the system. It deals with the direct behaviour of the hardware and software system and with the implementation and use of security mechanisms, logging features etc.

T. Technical level

Experiments in this class deal with the low-level design issues of operating systems and data security mechanisms, such as the internal structure of a reference monitor or an authentication protocol.

Taking all the above into consideration, we suggest that all the experiments in the field of teaching data security should be classified by a three-tuple

{X,Y,Z}, where:

- *X* denotes the degree of applicability (possible types: *D, L* and *F*)
- *Y* denotes the degree of innovation required (possible classes: *U, E, R* and *N*)
- *Z* denotes the level of generalisation of the experiment (possible levels: *M, S* or *T*)

This way of classifying the experiments allows us to generate 36 different classes of experiments. Introduction of a classification of this type is a necessity. Each of the classes requires different preparation and different backgrounds among students and lecturers. For example an experiment of a class *{D,U,S}, "demonstration of the use of an object on a system level"*, does not require students to have a great deal of knowledge, whereas participation in the *{F,N,T}* class, *"design of new technical tools in a real environment"*, demands a thorough knowledge of the discipline in order to yield substantial results.

4 EXAMPLES OF DATA SECURITY EXPERIMENTS

4.1 Introduction

The aim of this research is to systematise the role of experiments in teaching data security topics. Such a subject cannot be treated without presenting experiments already introduced by various university organisations. To do this we contacted about 30 universities on five continents, North America, Europe, Africa, Asia and Australia/Oceania, and asked about the contents of such experiments at their institutions. Our questionnaire is presented in Appendix 1. In this way we received information of about 15 - 20 different exercises/projects, which we believe is only a small part of the existing ones. Still, this may serve as a sample that can be used for illustrating the principle and give an idea of the range of experiments.

In this section we present examples of these experiments, apply the suggested classification terminology and make comments about them. All the experiments described below are currently being conducted at various universities.

Each experiment is classified, not only according to the taxonomy suggested in section 3, but also with respect to educational level, duration and the effort required (in man-hours) to perform the experiment:

{X,Y,Z}, educational level, duration, required effort

4.2 Experiment No 1: Eavesdropping techniques

Classification: {D,U,M}, graduate, 2 hours, 2 hours

This experiment aims to demonstrate problems related to eavesdropping techniques: measures and countermeasures.

Students have an opportunity to inspect real "bugs", i.e., "hidden" microphones of various types, and how they may be planted in office and home environments. Live demonstrations of devices that listen to analog and digital cellular phones and to pagers are parts of the demonstration.

On the countermeasure side, a non-linear detector is presented in action. A non-linear detector is a sensor that informs the operator as to whether there is a p-n junction (or semiconductor device) hidden within a radius of about 30 cm around the probe. The operation of a frequency analyser is also demonstrated. This device detects all radio transmission, and hence the presence of any radio-transmitting bugs. No preparation is required of the students prior to the demonstration.

4.3 Experiment No 2: Virus hunt

Classification: {D,U,S}, graduate, 2 hours, 2 hours

In this class, laptops are used to demonstrate typical virus activities (boot sector, stealth, polymorphic, macro etc). An analysis is conducted of the system's resources that demonstrates the existence of a virus. Virus detection and cleaning of software are also demonstrated.

Prior to the demonstration, students must attend a two-hour lecture on viruses and virus software, in which virus mechanics and various types of virus scanners are discussed.

4.4 Experiment No 3: Evaluation of system security by means of synthetic intrusions

Classification: ranging from {L,U,S} to {L,R,T}, undergraduate, about 4 weeks, 40-80 hours

The idea behind this project is to increase students' awareness of security by means of letting them find out for themselves how insecure a system can be, which unfortunately is true for many "normal" systems, i.e., systems in which security is not enhanced and thoroughly managed. The students start the project with no special security knowledge. In many cases they do not even know very much about the object system. Their task is to perform as many intrusions as possible and to report *how* they made them and *how much effort* was required in order to achieve the intrusions.

The results of the experiment are also used for research purposes, in particular to investigate methods for modelling and quantifying the intrusion process. Thus, owing to the requirements of this research, no specific time limit for the duration of the experiment is given, but it is implicit that the expected number of man-hours should normally fall in the range of 40 to 80 hours. The experiment requires careful supervision by a supervisor who must ensure that the experiment is carried out in a realistic way, but without disturbing other users or attempting something that would be illegal or unethical.

The outcome of the project is very dependent on the students involved. An interested and skilful student may very well start to develop new program tools, whereas some students may limit themselves to finding and using existing tools for the attempted intrusions. This is the reason why the classification would include classes such as *{L,U,S}*, *{L,E,S}* and *{L,R,S}* to *{L,U,T}*, *{L,E,T} and {L,R,T}*.

Each student (or group of students) summarises the results of the work in a *final report,* in which all successful intrusions are listed together with the expended effort. The students may also give their personal comments to the experiment, suggest improvements to the system as a result of their experience etc.

4.5 Experiment No 4: Demonstration of cryptological weaknesses

{L,U,T}, undergraduate, 4 hours, 4 hours

The students are presented with encrypted texts and a list of encryption methods, together with some tools for statistical analysis. Each text is encrypted with a different algorithm, but the students have no prior information about which algorithm is used on a specific text.

Statistical tools and other relevant methods, such as the Berlekamp-Massey algorithm, are used to perform a cryptanalysis of the text. The students are supposed to return the key and plaintext to show that they have been successful in the cryptanalysis.

4.6 Experiment No 5: Implementation of cryptographic algorithm

Classification: {L,R,S}, undergraduate, 4 weeks, 32 hours

The students are given the task of writing a program that implements a known cryptographic algorithm, such as a poly-alphabetic one or columnar transpositions. Furthermore, a brief user's manual is written. The function of the program developed is proven by means of demonstrating its function to the teacher and submitting the user's manual.

4.7 Experiment No 6: Data security audit

Classification: {F,R,M} or {F,E,M}, graduate, 3 months, about 100 hours

In this experiment students are required to perform a security audit of a real business organisation. The work is very closely supervised by the staff. In practice the supervisor is a member of the working team. The experiment is divided into three phases:

I. Preparation

Students undergo intensive training on how to perform a security audit. The exercise is the capstone of their two year study of Information Systems. The training includes familiarisation with the auditing methodology and method of conducting an interview.

The management of the organisation to be audited is contacted and permission is obtained to do the audit. Also, if necessary, security formalities are completed (e.g. issuing of badges, signing of nondisclosure certificates etc)

II. Data collection

Data is collected in three ways: personal interviews, reading related documents and observation. All personal interviews are presented for authorisation after the collection.

III. Data analysis

The data analysis usually contains two types of evaluation: consequences and recommendations. In the first part the team states what could happen if the discovered threat were not eliminated and an attack was launched against the organisation. The second part discusses ways of eliminating the security hole.

The final report has a professional appearance and is signed by the members of the research team, including the supervisor. The report is presented to the company as an official university document. The recipients of the reports normally treat them very seriously and in many cases try to implement the recommendations.

5 A PRELIMINARY EVALUATION OF THE DATA

Even though the received material is not large enough to be statistically significant, we have made a brief evaluation of it to see whether there is a tendency towards specific classes of experiments. One of the problems in this work is that some of the larger experiments contain elements of more than one class, e.g., experiment numbers 3 and 6, and may thus be regarded as multi-class experiments. In general, the distribution over the classes will be different if all the classes in a multi-class experiment are considered instead of identifying only one class, e.g., the most common one, in each experiment. However, a good correlation was found between the two ways of calculating, at least with the material available so far. The results below are thus valid for both cases.

In the applicability class, it turns out that laboratory experiments, coded *{L,*,*}*, are by far the most common. Three experiments of four belong to this class. This may not be very surprising, since the laboratory is the traditional place for conducting experiments, although it could have been thought that security experiments might have been an exception to this.

As regards the innovation class, there is a tendency towards an even spread between "use of" or "redesign of" the object, i.e., *{*,U,*}* or *{*,R,*}*, whereas "evaluation of" the object, *{*,E,*}*, is less common and "design of new improved objects", *{*,N,*}*, is quite infrequent.

The most common level of generalization for the experiments is the system level, *{*,*,S}*, which is as common as the two other groups, *{*,*,M}* and *{*,*,T}*, together. Obviously, it is easier or more natural to develop experiments which are on the system level, and thus more or less directly referring to the user, than to go up or down in the hierarchy. The management level would require an overview and the technical level a knowledge of details not shared by all students. A plausible interpretation of this fact is that business and management educations have a focus on the management level and vice versa.

In summary, the most "typical" experiment is an *{L,U,S}* or *{L,R,S}*, and these two classes together amounted to almost half of the total number.

Another completely different observation may be made. Although it may not be entirely evident from the above examples, we can conclude, on the basis of the full material received that this type of experimentation is very much in line with present trends in engineering education. Not only is it a good example of action learning, as mentioned in section 2, but it also incorporates substantial elements of innovative teaching and interdisciplinary approaches, as discussed in (Smith 1991) and (Yngström 1996).

6 DISCUSSION AND FUTURE WORK

While the present analysis covers most of the classes introduced in the taxonomy - from demonstrations conducted during regular lectures to substantial field work involving close co-operation with industry or other external organisations - it is not surprising that a vast majority of the experiments were performed in laboratories and aimed at redesigning or using well-known objects. Here, an interesting question is whether this outcome reflects an optimal set-up of experiments or is the result of some other condition, e.g., that the experiments carried out are simply those that were easiest to organise. We suggest that future investigations attempts to clarify this issue. Another related issue would be to establish the results of the experiment, preferably in quantitative terms, such as student satisfaction or learning effect. It is clear that there are a number of factors that might influence the result and that must be considered.

Examples are:

- attitude of students and staff towards conducting the experiments.
- quality of the experimental leader (e.g., staff, students, expert, tutor etc.)
- level of studies and the number of IS papers offered in the programme.

Finally, we would like to point out that the descriptions we received of experiments carried out at various universities are very interesting and should be made available to all information security educators. We suggest establishing a databank for the collection of descriptions of such experiments.

7 CONCLUSIONS

This paper is a first attempt to present a rationale behind enhancing data security studies with experimentation. Also, a classification method was developed and typical experiments presented and classified. The results so far are quite rewarding. Still they call for further research to be undertaken, both to gain a better understanding of the experimental process as such and to put it into an educational context.

8 ACKNOWLEDGEMENT

We would like to thank all of our contributors without whose help this research would not have been possible. The page limit of the paper prevented us from incorporating all experiments.

9 REFERENCES

(ERASMUS 1995) Gritzalis, D. (Ed), *University Programmes on Information Security, Dependability and Safety*, European Commission, Erasmus ICP, Projekt ICP-94(&95)-G-4016/11, Report IS-CD-3c, Athens, July. 1995.

(ERASMUS 1995b) Katsikas, S., Gritzalis, D. (Eds), *A Proposal for a Postgraduate Programme on Information Security, Dependability and Safety (Syllabus)*, Version 2.2, European Commission, Erasmus ICP-94(&95)-G-4016/11, Report IS-CD-4a, Athens, Sept. 1995.

(Kolb 1994) Kolb, D. Experiential Learning, Experience as the Source of Learning and Development, Prentice-Hall (1984).

(Muftic 1989) Muftic, S.: Security Mechanisms for Computer Networks, Ellis Horwood Ltd, England, ISBN 0-7458-0613-9, 1989.

(Pfleeger 1989) Pfleeger, C. P.: Security In Computing, Prentice Hall International, Inc. ISBN 0-13-799016-2, 1989.

(Revans 1984) Revans, R., The Sequence of Managerial Achievement, MCB University Press, Bradford (1984).

(Revans1992) Revans, R., The Origins and Growth of Action Learning, Chartwell-Bratt Lty, Bromley (1982).

(Smith 1991) Smith, R. A. (Ed.), "Innovative Teaching in Engineering", Ellis-Horwood (1991). ISBN 0-13-457607-1. pp. 3-40, 253-294.

(Yngström 1996) Yngström, L., IT Security and Privacy Education. In Proc. of the 12th International Information Security Conference, IFIP/SEC'96, Samos, May 21-24, "Information Systems Security: Facing the information society of the 21st century". Chapman&Hall. ISBN 0-412-78120-4. pp. 351-364.

(Zuber-Skerritt 1990) Zuber-Skerritt, O., Action Research For Change and Development, Centre for the Advancement of Learning and Teaching, Griffith University, Brisbane (1990).

Appendix: Questionnaire.

To: Teachers of Computer Security and other interested parties,
RE: Request for data on practical security experiments

[General information on the research project - not included]

****

DATA SECURITY EXPERIMENT

University.....
Faculty.....
Department.....
Course name.....
Course level (undergraduate, graduate, etc).....

Experiment type (please circle) DEMO LAB FIELD

Experiment duration (in min, hours, days, etc).....

Experiment goal.....
.....

Experiment description.....
.....

Assessment method (if appropriate).....
.....

****